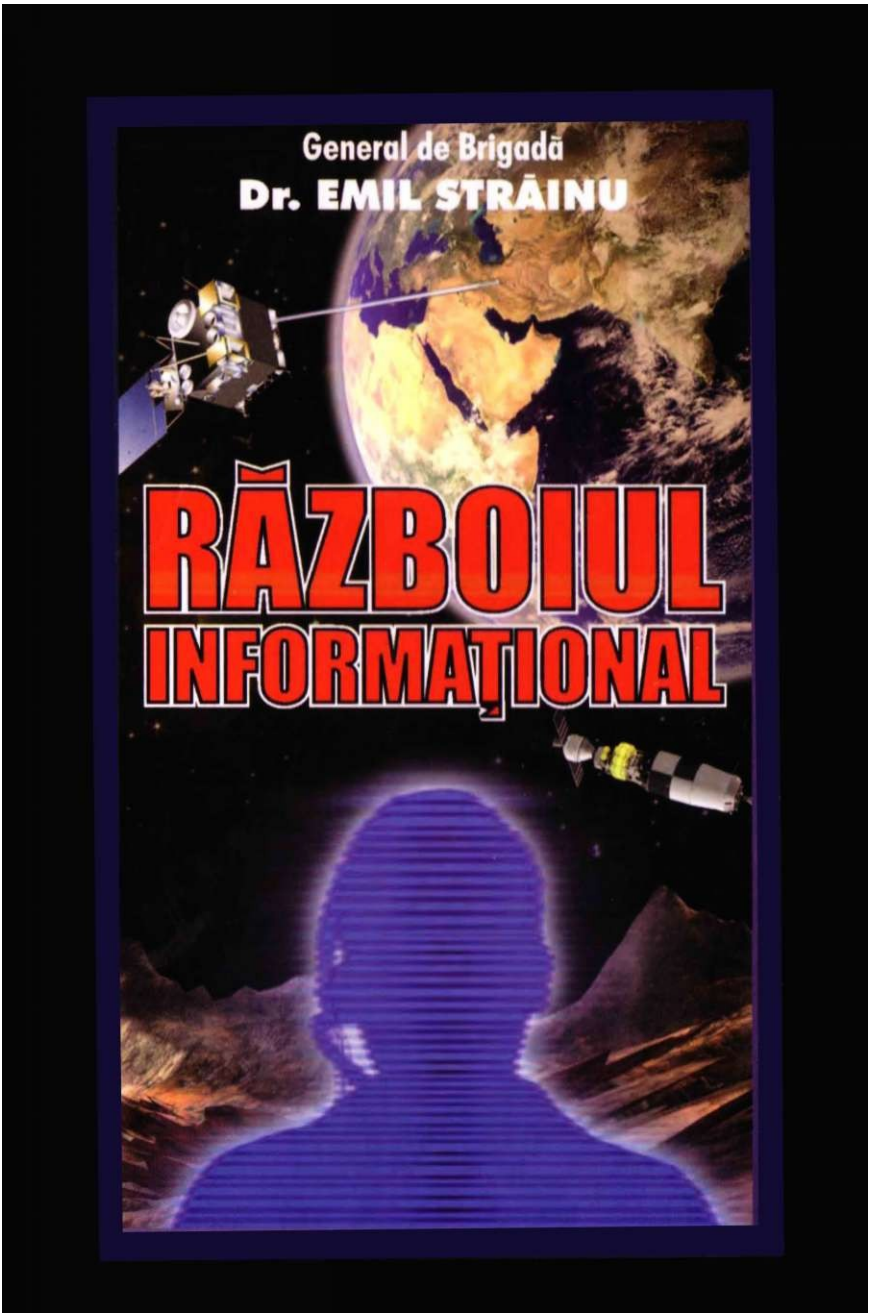

General de Brigadă
Dr. EMIL STRĂINU
RĂZBOIUL
INFORMAȚIONAL

Un simplu program aflat pe piaţă poate transforma orice computer personal într-o *unealta de spionaj*; INTERNETUL nu mai este de mult numai un mijloc de informare şi documentare, principalele sale actuale atribute sunt *manipularea*, *dezinformarea şi intoxicarea internauţilor*;

Există date potrivit cărora din orice punct de pe glob, folosindu-se un anume program ce declanşează un virus specializat, *un duşman ne poate ucide la comandă* prin intermediul PROPRIULU I computer dacă suntem „ţintă” şi ne aflăm în faţa ecranului cuplaţi la INTERN ET provocânduni-se instantaneu atac cerebral sau infarct!!; Telefonul mobil nu este altceva decât un terminal de computer prin care *putem fi oricând manipulaţi şi spionaţi* chiar dacă este „închis”;

INTERNETUL, telefonia mobilă şl suporţii informatici (dischete, Zip, CD, DVD, stick) sunt în mod activ şi curent folosiţi ca *purtători de mesaje subliminale* încă din fabricaţie s^u de la momentul încărcării cu filme, programe, instrucţiuni, etc.

General de brigadă dr. Emil Străinii
RĂZBOIUL INFORMAŢIONAL
?
Mică Enciclopedie
Coperta: DEIMOS IMAGE
Descrierea *CSP* a Bibliotecii Naţionale a României

STRÄINU, EMIL, Războiul Informa^onal / Strâinu Emil. — Bucureşti Solaris Prinţ, 2009
ISBN 978-606-92077-3-4
ISBN 978-606-92077-3-4 Copyright© 2009 SOLARIS'PRINT

General de brigadă dr. Emil Străinu
RĂZBOIUL
INFORMAŢIONAL
»
Mică Enciclopedie

Editura SOLARIS PRINŢ BUCUREŞTI – 2009
Coordonatorul lucrării: Psihosociolog Cornelia Prioteasa Consilier Ştiinţific: Prof.oniv Ghcorghe Butacaru
Motto:
O informaţiepe care o ai nu este cea pe cârc o vrei O informaţie pe care o vrei nu este cea de care ai nevoie
O informaţie de care ai nevoie nu este cea pe care o poţi obţine
O informaţie pe care o poţi obţine costă mai mult decât poţi să plăteşti
MURPHY (Legile informaţiei)
PREFAŢĂ
Analiza tipurilor de agresiuni* la care a fost/este supusa ţara noastră în prezent duce la oncluzia că cel mai grav fenomen cu care ne confruntăm acum (mai grav chiar decât cele din sfera economică) este un *complex proces de destructurare a realităţii etnice româneşti*.
Prin aceste acţiuni se urmăreşte lovirea şi alterarea/ distrugerea celui mai intim şi preţios filon al naţinuii române – Fiinţa Naţională
Autorii sunt state, corporaţii transnaţionale, grupuri şi grupări de interese mai mult sau mai puţin oculte, unele acţionând la vedere altele în ascuns, chiar şi de pe teritoriul naţional.
Mijloacele de atac sunt unele „domestice" ce acţionează „pe faţă", cum sunt mass-media şi internetul

cât şi altele conspirate ce ţin de modul de operare al serviciilor speciale şi agenţiilor secrete de informaţii.

Căile de atac sunt cele specifice războiului informaţional, războiului imagologic, războiului psihologic şi nu în ultimul râûd războiului psihotronic.

Pentru cunoaşterea şi identificarea unora dintre cele mai utilizate forme şi procedee de ducere a războiului informaţional am străns în prezentul volum păreri şi concepţii ale unor specialişti de marcă în domeniu.

Prezenta lucrare are un caracter de referinţă şi adună la un loc unele din cele mai semnificative tendinţe şi orientări actuale şi de perspectivă din domeniul războiului informaţional.

4 Vezi despre agresiuni geofizice (Canalul Bâstroe, de exemplu) agresiuni ce ţin de războiul climatic, agresiuni meteorologice, etc.) în Războiul Geofizic, Editura Solaris, Bucureşti 2009, etc. Agresiuni de tip psihotronic în Războiul Psihotronic, Editura Solaris, Bucureşti, 2009.

Oficial, conceptul de război electronic (R.I.) a fost lansat în Statele Unite, în decembrie 1992 (la aproape doi ani de la Războiul din Golf, considerat a fi „războiul pilot” în care s-au folosit mijloace specifice R.I.).

În septembrie 1995, Departamentul Apărării al SUA, a publicat prima definiţie oficială a războiului informaţional: „Războiul informaţional reprezintă acţiunile întreprinse pentru a obţine superioritatea informaţională, prin afectarea informaţiilor adversarului, a proceselor şi sistemelor informaţionale, în paralel cu acţiunile întreprinse pentru a apăra propriile informaţii t procese şi sisteme informaţionale.”

Multora dintre noi le este încă în minte transmisia în direct a războiului din Golf de către reţeaua de televiziune americană CNN. Dar să nu uităm şi de transmisia în direct la Televiziunea Naţională a Revoluţiei Române din Decembrie 1989.

Pentru specialişti, jurnalişti dar şi pentru publicul larg prezentul volum deschide noi orizonturi ale cunoaşterii realităţii actuale, confruntate cu numeroase

provocări nonconvenţionale şi asimetrice printre care şi cu un nou tip de război: Războiul Cunoaşterii...

Dr. Emil Ştrăinu

BAZELE RĂZBOIULUI INFORMAŢIONAL

ERA INFORMAŢIEI

Ronald R. Fogleman* Sheüa E. WidnalT

Competiţia pentru informaţie este la fel de veche ca şi conflictele umane. Este o caracteristică virtual definitorie a umanităţii. Naţiunile, corporaţiile şi indivizii caută, fiecare, să-şi mărească şi să îşi protejeze depozitul propria de informaţii, în timp ce încearcă să îl penetreze pe cel ai adversarului. Aproximativ din 1970 au avut loc îmbunătăţiri extraordinare în mijloacele tehnice de colectare, stocare, analizare şi transmitere a informaţiilor.

Au fost scrise topuri întregi despre impactul acestei revoluţii tehnice asupra conducerii războiului, în special de la „*Furtuna în Deşert***. Totuşi, majoritatea acestor lucrări se concentrează, în principal, asupra dezvoltărilor tehnice, nu asupra modului în care aceste dezvoltări au impact asupra doctrinei.

Acest material va formula întrebări importante pentru strategii US Army şi Air Force şi va da răspunsuri ferm bazate pe definiţii concise, experienţă instituţională şi pe concepte doctrinale.

În acest proces se va clarifica de ce competiţia pentru informaţii, care a apărut în zorile istoriei, este dintr-o data un subiect central al siguranţei naţionale. Mai aproape de casă, acest domeniu va descrie, de asemenea, modul în care ar trebui să evolueze doctrina Air Force şi US Army pentru a face faţă

4 General, USAF, Chief of Staff „ Secretary of the Air Force războiului informaţional. Scopul final este o fundamentare seriosă pe care să se bazeze inevitabilele schimbări în organizarea, pregătirea, dotarea şi mobilizarea forţelor şi capacităţilor militare. Deoarece are loc o revoluţie tehnologică[1] penetrând în forţă prin

1[1] Baza tehnologică a sistemelor informaţionale s-a schimbat radical din 1970. Aceste schimbări includ creşterea capacităţii de

sistemele informaţionale şi prin integrarea lor în viaţa noastră de zi cu zi şi ducând la termenul *„Era informaţiei”*.

Tehnologiile legate de informaţii concentrează date, măresc imens viteza de prelucrare şi transmitere a datelor şi asociază intim rezultatele în aproximativ orice aspect al vieţilor noastre. *Era informaţiei* transformă toate operaţiunile militare prin faptul că furnizează comandanţilor informaţii fără precedent din punctul de vedere al cantităţii şi calităţii[2]. Comandantul, care are avantajul în ceea ce priveşte observarea spaţiului de luptă, analiza evenimentelor şi distribuirea informaţiilor, posedă un puternic, dacă nu decisiv, avantaj ţn raport cu adversarul.

Înainte de a continua, trebuie să facem distincţia între *războiul epocii informaţionale* şi *războiul informaţional*. Facem această distincţie deoarece majoritatea literaturii tratează războiul informaţional şi progresele în tehnologia informaţiei sinonim.

Războiul epocii informaţionale foloseşte tehnologia informaţională ca pe o unealtă de a asigura economii, fără precedent de timp şi forţe, în operaţiunile noastre de luptă. În ultimă instanţă, războiul epocii informaţionale va afecta *toate* operaţiunile de lupta3.

Prin contrast, războiul informaţional, subiectul acestui document, vizualizează informaţia în sine ca pe un domeniu separat, o armă puternici şi o ţintă operativă.

Informaţia, după cum vom arăta în cele ce urmează, este dependentă de tehnologie. Totuşi, tehnologia erei informaţionale transformă în fapte o posibilitate teoretică:

---

stocare, a vitezei de accesare, vitezei de execuţie a instrucţiunilor şi vitezelor de comunicare. Datorită acestor schimbări, sistemele informaţionale penetrează în viaţa noastră. Considerăm aceasta ca fiind dovada prima facie a unei revoluţii. Totuşi, acest capitol nu intenţionează să răspundă întrebării daca aceste schimbări constituie o revoluţie sau măcar o evoluţie.

2 Aici, conceptul de calitate se refera la oportunitate, specificitate şi concreteţe.

manipularea *directă*[3] a informaţiilor adversarului. Acesta este firul conducător al acestui document.

CE ESTE INFORMAŢIA? Această întrebare este elementară, dar crucială. Este imposibilă discutarea coerentă despre războiul informaţional fără a defini riguros conceptul central: informaţia.

Informaţiile derivă din fenomene. Fenomenele, faptele sau evenimentele observabile, sunt *tot* ce se întâmplă în jurul nostru. Pentru a deveni informaţii, fenomenele trebuie percepute şi interpretate. În consecinţă, informaţiile sunt rezultatul a două elemente: fenomenele (datele) percepute şi instrucţiunile necesare pentru a interpreta aceste date şi a le da sens.

Această distincţie este importantă şi poate fi uşor sintetizată într-un paradox familiar: dacă un copac cade, dar nu e nimeni în împrejurimi ca să audă această cădere, a făcut zgomot? Copacul în cădere a cauzat unde de presiune în atmosferă, un fenomen. Zgomotul, informaţia denotând căderea copacului, survine atunci când urechea cuiva detectează undele de presiune, creând date, şi instrucţiunile creierului manipulează datele în sunetul care poate fi recunoscut ca un copac în cădere dacă nu exista o persoană care să îl audă (sau să îl vadă).

Fenomenele devin informaţii prin observaţie şi analiză. Prin urmare, informaţiile sunt o abstracţie a fenomenelor. Informaţiile sunt rezultatul percepţiilor şi interpretărilor noastre, indiferent de mijloace. După cum exemplifica cu claritate copacul în cădere, definirea informaţiei presupune două caracteristici:

Informaţia: *date şi instrucţiuni*.

Reţineţi că definiţia este distinctă pentru informaţii şi pentru tehnologie. Totuşi, ce putem face cu informaţiile şi cât de repede o putem face, este *foarte* dependent de tehnologie. Tehnologia dezvoltă dramatic mijlocele noastre observaţionale, dezvoltă şi concentrează depozitele de

3 Manipularea directă modifică informaţiile adversarului, în timp ce ocoleşte perspectiva adversarului, analitică sau procesul deciziei.

date şi accelerează prelucrarea instrucţiunilor. Folosim termenul următor pentru a circumscrie elementele dependente de tehnologie asociate cu informaţiile:

Funcţia informaţională: *orice activitate presupunând achiziţia, transmisia, stocarea şi procesarea informaţiilor*.

De exemplu, sistemul care spune unei maşini să stanţeze optzeci de capace de butuc realizează o funcţie informaţională. Presa de metal care le stanţează nu o face.

După cum s-£ menţionat anterior, comandantul, având informaţii mai bune, deţine un avantaj asupra adversarului. Operaţiunile militare formulează cereri speciale de funcţii informaţionale, căutând să-i dea comandantului un avantaj informaţional.

Supravegherea şi recunoaşterea sunt puterile noastre de observaţie. Inteligenţa şi analiza vremii sunt bazele pentru orientarea observaţiilor. Folosim aceste baze pentru a forma un „Air Tasking Order”, care comandă şi conduce operaţiunile de execuţie şi monitorizare în dirijarea conflictului. Navigaţia de precizie facilitează îndeplinirea misiunii. Împreună, acestea sunt tipurile de funcţii informaţionale militare care facilitează *toate* operaţiunile militare. Folosim termenul colectiv de funcţii informaţionale militare pentru a descrie funcţiile informaţionale de stimulare a forţei.

Funcţii Informaţionale Militare: *orice funcţie informaţională sprijinind şi facilitând mobilizarea forţelor militare*.

Această definiţie serveşte la delimitarea funcţiilor informaţionale militare importante de universul total al funcţiilor informaţionale.

La nivel de înaltă strategic, naţiunile urmăresc să obţină, exploateze şi protejeze informaţiile în sprijinul obiectivelor lor. Această exploatare şi protecţie poate avea loc de exemplu în arenele economice, politice sau militare. Cunoaşterea informaţiilor adversarului este un mijloc de dezvoltare a capacităţilor proprii, de degradare sau contracarare a capacităţilor inamicului şi protejare a activelor proprii, *inclusiv propriile informaţii*.

Asta nu e nou. Efortul de descoperire şi exploatare a informaţiilor a început de prima dată de când un grup de oameni a încercat să dobândească un avantaj asupra altuia.

Războiul informaţional constă din vizarea informaţiilor şi funcţiilor informaţionale ale inamicului, protejându-le pe ale noastre, cu intenţia de a deteriora voinţa sau capacitatea de luptă a acestuia.

Concentrându-ne asupra informaţiilor şi funcţiilor informaţionale, definim războiul informaţional ca:

Războiul Informaţional: *orice acţiune de refuz, exploatare, corupere şi distrugere a informaţiilor şi funcţiilor inamicului; protecţia proprie împotriva acestor acţiuni şi exploatarea funcţiilor proprii informaţionale militare*[4].

Această definiţie este baza următoarelor aserţiuni:

Războiul informaţional este orice atac împotriva oricărei funcţii informaţionale, indiferent de mijloace. *Bombardarea unei centrale telefonice este război informaţional. La fel este şi distrugerea soft-ului acestei centrale.*

Războiul informaţional este orice acţiune de protejare a propriilor funcţii informaţionale, indiferent de mijloce. *Întărirea şi protejarea centralei împotriva atacului aerian este război informaţional. La fel este şi utilizarea unui program anti-virus pentru protejarea soft-ului instalaţiei.*

Războiul informaţional este un mijioc, nu o finalitate, în exact acelaşi mod în care războiul aviatic este un mijloc, nu o finalitate. *Putem folosi războiul informaţional ca un mijloc de dirijare a atacului strategic şi interdicţiei, de exemplu, exact la fel cum putem folosi războiul aviatic pentru a dirija atacul strategic şi interdicţia.*

Militarii au încercat întotdeauna să obţină sau să afecteze informaţiile necesare unui adversar pentru a-şi mobiliza efectiv forţele. Strategiile trecute se bazau, în

4 Această definiţie depinde numai de natura acţiunii, nu de cum aceasta este realizată.

mod tipic, pe măsuri de genul disimulare şi diversiune pentru a influenţa deciziile, afectând percepţiile factorilor de decizie. Deoarece aceste strategii au influenţat informaţiile prin procesul de percepţie, ele atacau *indirect* informaţiile inamicului. Adică, pentru ca diversiunea să fie eficientă, inamicul trebuia sa facă trei lucruri:

să observe diversiunea;

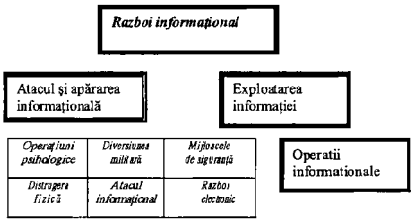
sa o analizeze ca realitate;

să acţioneze în baza ei, conform scopurilor, pentru care diversiunea a fost realizată.

Totuşi, mijloacele moderne de realizare a funcţiilor informaţionale conferă informaţiilor un plus de vulnerabilitate: accesul şi manipularea directă.

Tehnologia modernă permite acum unui adversar să schimbe sau să creeze informaţii fără a se baza pe observare şi interpretare. Iată o scurtă listă de caracteristici ale sistemelor informaţionale moderne creând această vulnerabilitate: stocarea concentrată, viteza de accesare, transmiterea dispersată a informaţiilor şi capacitatea sporită a sistemelor informaţionale de a dirija acţiuni într-o manieră autonomă. Măsurile inteligente de securitate pot reduce, dar nu pot elimina această vulnerabilitate; absenţa lor o face frapantă.

Militarii nu sunt înclinaţi să încredinţeze succesul lor în lupta norocului. Deci trebuie să ne dirijăm eforturile în războiul informaţional spre mai mult decât vizarea informaţiilor adversarului: trebuie şi să ne protejam informaţiile şi toate operaţiunile aferente. Air Force depinde esenţialmente de funcţiile informaţionale militare, ceea ce ne face vulnerabili la agresiunea informaţională. Integritatea funcţiilor noastre informaţionale militare, ca şi a informaţiei în sine, depinde esenţialmente şi în manieră directă de succesul operaţiunilor noastre militare.



Reamintindu-ne definiţia, războiul informaţional constă din activităţi care refuză, exploatează, corup, distrug sau protejează informaţiile. Mijloacele tradiţionale de realizare a războiului informaţional includ operaţiunile psihologice, războiul electronic, diversiunea militară, atacul psihologic şi diversele măsuri de securitate.

Operaţiunile psihologice *folosesc informaţiile pentru a afecta ra ţionamentuî inamicului*.

Războiul electronic *refuză inamicului informaţii corecte*.

Diversiunea militară *induce inamicul în eroare în ceea ce priveşte capacităţile sau intenţiile noastre*[5].

Distrugerea fizică *poate realiza războiul informaţional prin afectarea elementelor sistemului informaţional prin conversia energiei stocate în energie distructivă. Mijloacele de atac fizic variază de la bombe convenţionale până la arme cu impulsuri electromagnetice*.

Mijloacele de siguranţă *urmăresc să împiedice adversarul să afle despre capacităţile şi intenţiile noastre în plan militar*[6].

---

5 Diversiunea militară dă un excelent exemplu de cum acţiunile sunt definite de finalităţile lor nu de mijloace. Puterea aeriană poate conduce războiul informaţional prin diversiunea militară ca în operaţiunea "Fortitude North", din al doilea Război Mondial, unde persoane neidentificate au detonat două bombe în Pas de Calais, pentru fiecare bombă aruncată în Normandia, un efort de succes în inducerea în eroare a nemţilor în ceea ce priveşte planurile noastre de invazie.

6 Măsurile de securitate curente includ OPSEC, COMSEC şi COMPUSEC. Ca evoluţie a tehnologiei informaţionale, aceste măsuri de securitate mai mult ca sigur vor evolua în forme total

Era informaţiei a prevăzut mijloace noi şi practice pentru a refuza, exploata, corupe sau distruge informaţia, la fel ca vulnerabilităţile ce fac aceste atacuri posibile. Doctrina US Army şi Air Force nu cunoaşte şi nu defineşte aceste atacuri asupra informaţiei, pe care noi le numim *'atacul informaţional*'.

Atacul informaţional *degradarea directă a informaţiei fără schimbări vizibile a entităţii acesteia înăuntrul căreia se află*.

Atacul informaţional, constrâns de definiţia informaţiei, este limitat la modificarea directă a datelor şi instrucţiunilor. Este, prin urmare, tocmai un alt mijloc de conducere a războiului informaţional, unul a căror efecte imediate nu include schimbări vizibile a entităţii înăuntrul căreia aceasta se află.

Ca să spunem aşa, după ce a devenit subiectul atacului informaţional o funcţie informaţională nu se poate distinge de starea ei originală, decât prin verificarea datelor şi instrucţiunilor sale[7].

Aşa cum am descris anterior, există două căi de a influenţa funcţiile informaţionale ale adversarului: directă şi indirectă.

Războiul informaţional indirect afectează informaţia creând fenomene, pe care adversarul la va percepe, interpreta şi acţiona asupra lor.

Diversiunea militară, atacul psihic şi dezinformarea tradiţională îşi ating ţelurile indirect. De exemplu, ţinta decepţiei este de a determina adversarul să ia decizii incorecte; decepţia reuşind acest lucru prin crearea unei realităţi aparente.

În general, această substituţie crează fenomene pe care inamicul trebuie să le observe. Reuşita, oricum, depinde de câteva condiţii: adversarul, în realitate să observe fenomenul şi ulterior să îl transforme în date; să-l analizeze în informaţia dorită şi să acţioneze în baza

---

diferite.

7 Aruncarea unui magnet puternic, de către o echipă S OF asupra unui hard disc este un exemplu de atac informaţional.

informaţiei, în maniera dorită.

Războiul informaţional direct afectează informaţia prin modificarea componentelor sale, fără a se baza pe puterile adversarului de percepere şi interpretare. Atacul informaţional acţionează direct asupra informaţiei adversarului. De curând toate funcţiile informaţionale sunt însăşi controlate de informaţie, atacul informaţional putând fi direct împotriva celor mai multe funcţii informaţionale.

Războiul informaţional direct, centrul atacului informaţional, acţionează asupra informaţiilor adversarului, fără a se baza pe funcţiile de culegere, analiză şi decizie ale lui. Poate scurtcircuita bucla OODA[8] (Observaţie, Orientare, Decizie şi Acţiune) prin crearea unor observaţii şi perturbării orientării, sau o poate decapita prin impunerea unor decizii sau provocarea unor acţiuni. O scurtă ilustrare va servi pentru a demonstra diferenţa între aplicaţiile războiului informaţional direct şi indirect:

Scopul nostru, folosind diversiunea militară, este să facem adversarul să creadă că există o escadrilă de aparate de luptă acolo unde de fapt, nu este niciuna, şi să acţioneze, în baza acestei informaţii, într-o manieră benefică pentru operaţiunile noastre.

Războiul informaţional indirect: folosind diversiunea militară, putem construi piste false şi hangare false, şi să generăm alte activităţi suficiente pentru a prezenta o imagine convingătoare. Ne bazăm pe adversar să observe pseudo-operaţiunile de luptă şi să le interpreteze că fiind reale (contrar detectării lor ca false). Doar atunci aceasta devine informaţia pe care vrem ca adversarul să o aibă.

Războiul informaţional direct: în sens contrar, dacă

8 OODA: Observaţie, Orientare, Decizie si Acţiune. Observaţia transformă fenomenele în date. Orientarea procesează datele în informaţii. Decizia transformă informaţia în ordine. Acţiunea transformă ordinele în acţiune. Bucla OODA este continuă – atunci când acţionezi observi rezultalele începând procesul din nou.

folosim atacul informaţional pentru a crea escadrila de luptă în baza de informaţii a adversarului, rezultatul – decepţia – este precis acelaşi. Dar mijloacele acestui rezultat, care depind de resurse, timp şi nesiguranţă, sunt dramatic diferite.

Latura defensivă a măsurilor de securitate a războiului informaţional vizează protejarea informaţiei (previne ca un adversar să conducă cu succes războiul informaţional împotriva funcţiilor noastre informaţionale). Măsurile de securitate curente ca OPSEC şi COMSEC sunt mijloace tipice de prevenire, detectare şi răsturnare a acţiunilor indirecte ale adversarilor asupra funcţiilor noastre informaţionale.

În contrast, măsurile de securitate ca COMPUSEC includ prevenirea, detectarea şi răsturnarea acţiunilor informaţionale directe asupra funcţiilor noastre informaţionale. Măsurile de securitate viitoare trebuie să evolueze în raport cu progresele tehnologiei informaţionale. Consecutiv, noi măsuri vor lua probabil forme total diferite, de măsurile de securitate de astăzi, înrădăcinate în cerinţele de securitate anterioare.

Aşa cum demonstrează exemplul simplu din această lucrare, trebuie să evităm să cădem victima efectelor profunde şi păgubitoare ale războiului informaţional.

Din două motive. În primul rând, pentru că războiul informaţional oferă mijloace importante pentru îndeplinirea misiunilor forţelor aeriene, în al doilea rând, pentru că integrarea larg răspândită a sistemelor informaţionale în operaţiile forţelor aeriene transformă funcţiile noastre informaţionale militare într-o ţintă valoroasă. Un exemplu ipotetic folosind atacul informaţional arată cum războiul informaţional poate îndeplini o misiune tipică Air Force:

Interdicţia împiedică sau întârzie ajungerea resurselor esenţiale la unităţile combatante. În acest sens, o abordare constă în distrugerea podurilor de legătură folosind bombe ghidate cu laser. Ca alternativă, am putea să alterăm informaţiile logistice ale adversarului, marcând

în mod intenţionat eronat acele poduri ca fiind distruse, ceea ce determină factorii de planificare să redirijeze forţele şi resursele. Ambele modalităţi realizează acelaşi scop; atacul informaţional oferă posibilitatea de a ne expune activele unui atac.

Ca exemplu, evidenţiind necesitatea unei apărări robuste împotriva unei agresiuni informaţionale, imaginaţi-vă haosul care ar apare dacă un adversar ar reuşi să penetreze baza noastră de date cu alocare în timp a forţelor. Schimbări subtile în ea ar fi suficiente pentru a reduce aproape la zero capacităţile noastre de protecţie.

În prezent, doctrina US Army şi Air Force recunoaşte războiul aerian şi războiul spaţial. Totuşi, doctrina nu identifică misiuni separate pentru războiul aviatic sau războiul spaţial, în loc de asta, ambele interferează rolurile şi misiunile. Similar războiul informaţional nu poate fi clasificat ca o misiune singulară. A face aceasta ar însemna un eşec pentru integrarea completă a războiului informaţional în doctrina forţelor aeriene.

Să ne amintim că misiunile sunt sarcini operaţionale îndeplinite pentru obţinerea obiectivelor militare. Războiul aerian este un mijloc, definit de mediu, pentru executarea acelor misiuni. Există trei obiective ale războiului aerian:

controlul spaţiului aerian în timp ce protejăm forţele noastre de acţiunile inamicului;

exploatarea controlului aerian pentru angajarea forţelor proprii împotriva inamicului şi sporirea generală a eficienţei forţelor noastre.

În doctrina noastră, obiectivele controlului, exploatarea cât şi sporirea eficienţei se transpun în rolul spaţiului aerian, în acţiunea şi sporirea forţelor. În multe privinţe, informaţia poate fi considerată ca un domeniu aşa cum sunt uscatul, marea, aerul şi spaţiul.

Informaţia are caracteristicile[9] sale proprii de

9 Pământul, marea, aerul şi spaţiul sunt domenii înăuntrul carora noi putem desfăşura operaţii militare. Fiecare domeniu înăuntrul său impune asupra operaţiilor caracteristicile sale. Informaţia şi funcţiile sale, de asemenea, poate fi gazdă pentru operaţiile

mişcare, greutate şi topografie aşa cum spaţiul, aerul, marea şi uscatul au trăsăturile lor distincte. Există paralele conceptuale puternice între conceperea aerului şi informaţia ca domeniu.

Înaintea fraţilor Wright, aerul, care evident exista, nu era un teren propice pentru operaţiuni militare practice şi de anvergură. Similar, informaţiile existau înainte de epoca informaţională. Dar epoca informaţională a schimbat caracteristicile domeniului informaţiei ca operaţiunile militare de anvergură din interiorul ei să devină practice.

Războiul informaţional ca şi războiul aerian este mijlocul definit de domeniul în care urmează să fie executate misiunile militare. Există trei obiective ale războiului informaţional:

controlul domeniului informaţional în aşa fel încât să-l putem exploata în timp ce protejăm funcţiile noastre informaţionale militare, de acţiunile inamicului:

exploatarea controlului informaţional pentru angajarea războiului informaţional împotriva inamicului;

sporirea generală a eficacităţii forţelor prin dezvoltarea deplină a funcţiilor informaţionale militare.

Primul obiectiv al războiului informaţional, de a controla domeniul pentru ca să îl putem exploata în timp ce protejăm funcţiile noastre informaţionale militare de acţiunile inamicului, are o contribuţie semnificativă la controlul spaţiului de luptă.

În prezent, doctrina forţelor aeriene recunoaşte două misiuni pentru controlul spaţiului de luptă: antiaeriană şi antispaţială. Misiunile antiaeriene au ca obiective controlul aerului; misiunile antispaţiale au ca obiectiv controlul spaţiului. Claritatea şi consistenţa ne cer să numim acele activităţi, dedicate controlului informaţional, contrainformaţii.

Contrainformaţia: *acţiune dedicată pentru a controla spaţiul informaţional*.

În plus, contrainformaţia, la fel ca misiunile

---

militare, însă aceste operaţiuni trebuie să se conformeze cu caracteristicile sistemului informaţional şi funcţiilor sale.

antiaeriene şi antispaţiale, are atât aspecte ofensive cât şi defensive. Contrainformaţia ofensivă, ne face capabili să folosim domeniul informaţional şi îl face pe adversar incapabil sa-l folosească.

Mijloacele tipice includ, atacul fizic, diversiunea militară, operaţiile psihologice, războiul electronic şi atacul informaţional. Contrainformaţia defensivă, include atât acţiuni active cât şi pasive pentru a ne proteja de acţiunile războiului informaţional ale adversarului. Ea este realizată, de exemplu, prin apărarea fizică, securitatea fizică, OPSEC, COMSEC, COMPUSEC şi serviciile de informaţii.

Controlul aérospatial ne face capabili să folosim teritoriul aerului şi spaţiului fără să suferim pierderi substanţiale şi să producem pagube însemnate inamicului ce deţine aceste teritorii. Contrainformaţia în colaborare cu misiunile antiaeriene şi antispaţiale caută să creeze un astfel de mediu.

Al doilea obiectiv al războiului informaţional este să exploateze controlul nostru asupra informaţiei, în aplicarea războiului forţelor aeriene, misiunile de atac strategic, interdicţia şi susţinerea aeriană exploatează controlul aerian. Similar război informaţional ar putea fi folosit să realizeze aceleaşi obiective. Am citat deja un exemplu despre felul în care războiul informaţional poate realiza interdicţia. El, de asemenea, poate realiza atacul strategic.

Să presupunem că vrem să limităm mobilitatea pe termen lung a inamicului prin restricţionarea aprovizionării cu combustibil. În primul rând, îi identificăm rafinăriile, ca cea mai convenabilă ţintă de realizare a acestui ţel.

Prin cercetare, identificăm în continuare rafinăriile specifice care au cea mai mare capacitate de producţie. La fiecare rafinărie găsim că există un turn de cracare critică. Organizăm o lovitură şi cu o admirabilă economie de forţă, realizăm scoaterea din funcţiune a rafinăriilor prin distrugerea numai acelor turnuri în timp ce lăsăm restul neatins. Acesta este un exemplu clasic de atac strategic.

Aceeaşi situaţie. Ca în toate rafinăriile moderne şi acestea au vaste sisteme de control automat. Aceste funcţii informaţionale vaste oferă o ţintă potenţială pentru războiul informaţional. La începutul conflictului, noi am realizat o misiune contrainformativă ofensivă prin penetrarea şi caracterizarea sistemului de control automat al rafinăriei.

În acest proces, am descoperit câteva puncte informaţionale vulnerabile, care ne-au ajutat să stabilim mijloacele pentru afectarea operaţiunilor rafinăriilor, la o dată care rămâne la alegerea noastră. Mai târziu, în timpul conflictului, combinat cu interdicţia şi operaţiunile de la sol, alegem să exploatăm una dintre vulnerabilităţi. În acest fel, am scos din funcţiune rafinăriile lor. Şi'acesta este un exemplu clasic de atac strategic.

Tehnologia informaţională este deja puternic înglobată în operaţiunile noastre militare, punând la dispoziţie cantităţi inimaginabile de informaţii. Exploatând aceste informaţii avem la dispoziţie posibilităţi de lovire; bazându-ne pe acestea se creează inevitabil vulnerabilităţi, potenţiale deformaţii. Aceasta, combinată cu progresele atât în abilitate cât şi în localizarea şi distrugerea punctelor de comandă şi control (C2), fac C2 mai mult ca oricând o ţintă realizabilă.

Istoria a arătat că operaţiunile militare de succes pot realiza lovituri eficiente prin paralizarea abilităţii inamicului de a exercita comanda şi controlul. Aviatorii l-au considerat, întotdeauna un obiectiv important şi au depus eforturi mari împotriva C2in aceste două motive, eforturile pentru perturbarea şi distrugerea elementelor de comandă şi control ale adversarului ne-au determinat să identificăm o misiune separată în aplicaţiile forţelor.

Atacul C2: *orice acţiune împotriva oricărui element al sistemului de comandă şi control al inamicului*.

Al treilea obiectiv al războiului informaţional este dezvoltarea funcţiilor informaţionale pentru sporirea eficienţei tuturor forţelor. Anterior am descris funcţiile informaţionale militare ca un sprijin pentru angajarea

forţelor militare.

Doctrina noastră curentă nu include o astfel de misiune. Pentru a umple acest spaţiu gol, vom include operaţiile informaţionale în sporirea forţelor. Câteva exemple de operaţii informaţionale sunt: supravegherea, recunoaşterea, comanda şi controlul, comunicaţiile, identificarea conflictelor, inteligenţa, precizia zborului şi vremea.

Trăsătura distinctă a misiunilor operaţiunilor informaţionale este că se ocupă în primul rând cu informaţiile atât ca resurse cât şi ca produs.

Rolul şi misiunile puterii aerospatiale			
Controlul aerospaţial	Misiuni ale forţelor	Sporirea forţelor	Sp forţelor
Antiaerian	Atacul strategic	Transportul aerian	Ba & DEF
Antispatial	Interdicţia	Alimentarea în aer	Lo
Contra - informaţiile	Sprijinul aerian	Transportul în spaţiu	Sp
	Atacul CI	Operaţii speciale	Op al
		Operaţii informaţionale	Sp pe orbit

Operaţiile informaţionale: orice *acţiune presupunând achiziţia, transmisia, stocarea şi procesarea informaţiilor ce sporesc angajarea de forţe militare*.

Deoarece avem nevoie de informaţii relevante, veridice şi oportune pentru tot ceea ce facem, operaţiile informaţionale susţin conducerea misiunilor pe parcursul tuturor celor patru roluri, de la controlul aérospatial la sprijinul forţelor.

Operaţiile informaţionale asigură comandanţilor abilitatea să observe spaţiul de luptă, analiza evenimentelor şi forţele directe. Operaţiile informaţionale asigură logisticienilor abilitatea de a cunoaşte ce este în

dotare şi unde este necesar. Operaţiile informaţionale asigură conducerea zborului, abilitatea de a cunoaşte unde este ţinta, cum este apărarea ei şi să selecteze care este cea mai corespunzătoare armă.

În final războiul informaţional se interferează cu toate rolurile şi misiunile forţelor aeriene. Este un alt mijloc de conducere a misiunilor noastre tradiţionale. Oricum există trei sarcini operaţionale superioare prin care războiul informaţional ne face capabili sa executăm, ceea ce nu este convenabil tratat de către doctrina noastră actuală: contrainformaţia, Atacul C2 şi operaţiile informaţionale.

Similar, am hotărât să excludem două misiuni care nu mai sunt relevante potrivit regrupărilor misiunilor: războiul electronic, anterior cuprins în cadrul creşterii forţelor, care este acum însumat de către războiul informaţional; supravegherea şi recunoaşterea ce sunt considerate, acum, momente ale operaţiilor informaţionale.

Oricum, această listă nu este exhaustivă. Aşa cum am arătăt titlul acestui material, ideile conţinute vizează bazele şi nu întreaga construcţie. Invariabil, pe măsură ce forţele aeriene se acomodează în totalitate cu revoluţia tehnologiei informaţionale, se pot ridica sarcini operaţionale adiţionale care la rândul lor vor adăuga sau exclude unele misiuni.

În sens larg, aceste baze continuă să ofere un test veridic pentru războiul informaţional, toate noile misiuni având nevoie să îl susţină şi să îl treacă.

Focarul războiului informaţional este orice funcţie informaţională indiferent dacă este C2, un sistem de control al unei rafinării sau o centrală telefonică. C2 reprezintă numai o parte a universului funcţiilor informaţionale militare. Statul Major defineşte comanda şi controlul:

Comanda şi controlul: *exercitarea autorităţii şi direcţiei, de citre un comandant corespunzător desemnat asupra forţelor distribuite în îndeplinirea misiunii*.

Comanda şi controlul războiului (C2W) se adresează activităţilor directe împotriva abilităţii adversarului de a direcţiona dispunerea şi angajarea de forţe, sau acelora care protejează prietenoasa amabilitate a comandanţiilor să facă aceasta. Aşa cum am arătat, războiul informaţional nu atacă numai procesul C2 ci, de asemenea, puterea de luptă însăşi a inamicului.

Cu alte cuvinte, prin definiţie, C2W nu este asociat cu reducerea sau anularea abilităţii sau dorinţei unităţilor de luptă de a executa ordinele lor. Operaţiile psihologice tactice şi contramăsurile electronice de autoprotecţie afectează abilitatea unităţilor să execute ordinele.

Dar ele, în niciun caz, nu afectează abilitatea comandanţilor să emită ordine acelor unităţi şi nici abilitatea lor de a primi acele ordine. Deşi extraordinar de importantă, politica de comandă şi control a războiului este numai o aplicaţie particulară a războiului informaţional.

Pentru ca militarii să se concentreze numai asupra C2W, ar trebui să ignore alte ţinte legitime. Pentru aceasta războiul informaţional şi activităţile lui ajutătoare instruirea şi aspectele de dotare, sunt esenţiale ca C2W să fie deplin eficient.

Noi am stabilit că războiul informaţional este important pentru forţele aeriene din două motive. În primul rând, de când funcţiile noastre informaţionale militare reprezintă o ţintă valoroasă noi trebuie să facem eforturi importante de apărare. În al doilea rând, cum exemplele din această lucrare arată că războiul informaţional este un mijloc potenţial de realizare a misiunilor tipice forţelor aeriene: atacul strategic, interdicţia etc. Mai temeinic forţele aeriene deja produc războiul informaţional prin sisteme cum sunt EF-111 şi „Compass Call”.

Dar, într-un sens mai larg, războiul informaţional ar putea fi un mijloc de conducere a oricărei misiuni pe care serviciul deja o exercită – serviciul este în cea mai buna poziţie, ca să aleagă mijloacele cele mai bune pentru

finalizarea lor. Fiecare serviciu are cerinţele sale operaţionale unice.

În cele din urmă armata este cea mai calificată să decidă care mijloace sunt cele mai corespunzătoare pentru atingerea scopurilor pe care comandantul Statului Major le-a stabilit pentru armată. Ca un rezultat al expertizei unice a serviciului cerinţele proprii OODA, logisticii etc., fiecare serviciu are preocupări pentru războiul informaţional. În dezvoltarea construcţiei doctrinale în acest material am folosit terminologia şi exemplele forţelor aeriene.

Acesta este fondul nostru, aceştia sunt termenii şi spaţiul cu care suntem obişnuiţi. Dar argumentul pe care noi îl prezentăm nu este dependent de terminologie, înlocuirea termenilor forţelor aeriene, cu cei ai armatei ori ai marinei vor lăsa concluziile neschimbate.

CONCLUZII: Revoluţia informaţională, care a apărut rapid, nu arată semne de încetineală. În măsura în care forţele aeriene devin mai sofisticate din punct de vedere tehnologic, în aceeaşi măsură devin dependente tehnologic. Trebuie să folosim această sofisticată tehnologie pentru a beneficia de toate oportunităţile pe care informaţia le oferă ca ţintă.

De asemenea, trebuie să fim conştienţi că echipamentele noastre tehnice pot reprezenta o posibilă deformaţie vulnerabilă. Sistemele noastre robuste de apărare ale funcţiilor informaţionale pot reprezenta ceea ce ne face pe noi sa nu fi întâmpinat eşecuri militare.

Informaţia, combinată cu funcţiile informaţionale, are trăsături distincte care garantează ca să fie considerată un domeniu, la fel cum uscatul, marea, aerul şi spaţiul sunt domenii.

Războiul informaţional nu ocupă un loc minor în doctrina forţelor aeriene. La fel ca războiul aerian, războiul informaţional poate face parte din multe misiuni AFM l-l. La fel ca atunci când războiul spaţial a fost integrat în doctrina forţelor aeriene, tratarea informaţiei ca un domeniu, ne dă posibilitatea, acum, să adăugăm alte

misiuni:

Contrainformaţia: Acţiune dedicată pentru a controla spaţiul informaţional.

Atacul C2: Orice acţiune împotriva oricărui element al sistemului de comandă şi control a adversarului.

Operaţiile informaţionale: Orice acţiune presupunând achiziţia, transmisia, stocarea sau procesarea informaţiilor care implică mobilizarea forţelor militare.

De la primul Război Mondial, aviatorii au trebuit să controleze efectiv spaţiul aerian pentru a angaja puterea aeriană. Mai mult, superioritatea în aer şi spaţiu este virtual „sine qua non" pentru angajarea forţelor terestre şi navale. Informaţia este următorul domeniu pe care trebuie să-l controlăm pentru a opera eficient şi cu cea mai mare economie de forţe.

La începui am arătat că lupta pentru informaţii este atât de veche ca primul conflict uman. Ea implică creşterea şi protecţia stocului nostru de informaţii şi timp ce le penetrează şi limitează pe cele ale adversarului.

Recenta explozie în tehnologia informaţională îndeamnă punerea în discuţie a războitlui informaţional în şi din afara guvernului, ţintind funcţiile informaţionale ale inamicului, în timp ce le protejează pe ale noastre, cu intenţia de degradare a voinţei şi capacităţii sale de luptă.

Pentru aviatori, controlul spaţiului de luptă este misiunea nr. 1. Odată cu progresele în tehnologia informaţiilor, aviatorul trebuie să dovedească superioritatea în informaţii aşa cum au superioritate în aer şi spaţiu.

Numai cu aceste domenii sub controlul nostru putem efectiv angaja activele noastre. Funcţiile informaţiei militare sunt esenţiale pentru operaţiunile noastre de luptă, ele sunt un instrument de realizare a obiectivelor comandantului Forţelor Unite. Ţintind funcţiile informaţionale ale adversarului îl împiedicăm să şi le realizeze.

În această lucrare am expus buzele doctrinei războiului informaţional. Scopul nostru este să oferim o

bază larg acceptată pentru adoptarea doctrinei forţelor aeriene la epoca informaţională. Ultima ţintă? Să încorporam războiul informaţional în felul în care Air Force organizează, antrenează, echipează şi acţionează.

Definiţii

Atacul C2: Orice acţiune împotriva oricărui element al sistemului de comandă şi control al adversarului.

Comandă şi control: Exercitarea autorităţii şi direcţiei, de către un comandant corespunzător desemnat asupra forţelor distribuite în îndeplinirea misiunii.

Contrainformaţia: Acţiune dedicată pentru a controla spaţiul informaţional.

Contrainformaţia defensivă: Acţiune ce protejează funcţiile noastre militare de adversar.

Războiul informaţional direct: A schimba informaţia adversarului prin crearea de fenomene fără a implica intervenţia funcţiilor perceptive şi analitice.

Războiul informaţional indirect: A schimba informaţia adversarului prin crearea de fenomene pe care adversarul trebuie să le observe şi să le analizeze.

Informaţia: Date şi instrucţiuni.

Atacul informaţional: Degradarea directă a informaţiei fără schimbări vizibile a entităţii acesteia, înăuntrul căreia se află.

Funcţia informaţională: Orice activitate presupunând achiziţia, transmisia, stocarea şi procesarea informaţiilor.

Operaţiile informaţionale: Orice acţiune presupunând achiziţia, transmisia, stocarea sau procesarea informaţiilor care implică mobilizarea forţelor militare.

Război informaţional: Orice acţiune de refuz, exploatare, corupere şi distrugere a informaţiilor şi funcţiilor inamicului; protecţia proprie împotriva acestor acţiuni şi exploatarea funcţiilor informaţionale militare.

Funcţii informaţionale militare: Orice funcţie informaţională sprijinind şi facilitând mobilizarea forţelor militare.

Contrainformaţia ofensivă: Acţiune împotriva funcţiilor informaţionale ale adversarului.

RĂZBOIUL INFORMAŢIONAL DEFENSIV

DAVID S. ALBERTS*

Războiul informaţional a devenit sinonim cu revoluţia în tehnologiile informaţionale şi cu potenţialul acestora de a transforma strategii militare şi capabilităţi. Există un consens în privinţa ideii potrivit căreia prosperitatea naţională, dacă nu chiar supravieţuirea, depinde de abilitatea noastră de a dezvolta efectiv tehnologia informaţională. Fără să fim capabili să apărăm informaţia vitală, procesele şi sistemele informaţionale, o astfel de strategie este sortită eşecului.

RI este adesea considerat ca fiind definit de un set particular de ţinte – factori de decizie, informaţie, procese şi sisteme informaţionale. Asocierea spaţiului de conflict („battlespace") şi a RI este în constantă creştere, depăşind situaţiile militare tradiţionale. În unele medii, RI este asociat cu creşterea tehnologiilor informaţionale, pentru a obţine o eficienţă sporită.

Acest lucru a lărgit la maxim înţelesul conceptului de RI şi a semănat multă confuzie. Pentru acest motiv, în materialul de faţă, sintagma „strategii informaţionale" se referă la recunoaşterea şi utilizarea informaţiei şi tehnologiei informaţionale ca instrument de putere naţională, care poate fi independent de, sau complementar cu, prezenţa şi operaţiile militare.

Întinderea sau spaţiul de conflict, al strategiei RI, poate fi definită de jucători şi de cele trei dimensiuni – natura, nivelul şi Zonele interacţiilor lor (Figura 1). Statele nu sunt singurii jucători. Actorii non-statali (grupuri politice, etnice şi religioase, crima

Institutul de Studii Naţionale Strategice,* Universitatea Naţională de Apărare Washington D.C.

Organizată organizaţii internaţionale şi transnaţionale, persoane care au &cces la tehnologia informaţională etc.) sunt apţi să angajeze atacuri informaţionale şi să dezvolte strategii informaţionale pentru a-şi atinge scopurile. În ultima vreme, termenul de „război" a fost folosit destul de neglijent (exemple:

Războiul Sărăciei, Războiul Drogurilor, Războiul Crimei), însă acest lucru nu trebuie să surprindă. RI a evoluat în ultimii ani şi a devenit un termen atotcuprinzător, referindu-se la activităţi disparate, unele dintre ele fiind de mult timp asociate ideii de competiţie, de conflict şi de război.

Acestea includ activităţi mergând de la campanii de propagandă (incluzând războiul mass-mediei) la atacuri (fizice sau nu) contra comandanţilor, surselor lor de informare, şi mijloacelor de comunicare cu forţele lor. Sub această umbrelă largă, cunoscută ca fiind RI, putem găsi activităţi ce sunt asociate cu concepte şi operaţii militare, incluzând înşelătoria, războiul de comandă şi control (C2W) şi operaţii psihologice (Psyops). Progresele tehnologice au adăugat noi forme de război: războiul electronic (EW) şi războiul hackerilor.

Termenul de „Război informaţional defensiv" (RI-D) se referă la toate acţiunile întreprinse pentru a se apăra împotriva atacurilor informaţionale (atacuri asupra factorilor de decizie, informaţiei, proceselor informaţionale şi mijloacelor de comunicare a deciziilor lor). În sens strict, din moment ce aceste atacuri pot fi lansate pe timp de pace către ţinte civile de către grupuri care nu sunt militare, atât străine cât şi autohtone, în loc de RI-D ar trebui să se utilizeze termenul de „Strategie a Războiului informaţional defensiv".

Această privire de ansamblu, asupra RI-D, nu încearcă să rezolve problemele apărării împotriva diferitelor tipuri de atacuri informaţionale, ci mai degrabă doreşte să focalizeze atenţia pe subsetul RI, care implică atacuri asupra structurii noastre informaţionale, incluzând ceea ce a devenit cunoscut ca fiind „războiul hackerilor", şi în forma sa mai serioasă, „războiul digital".

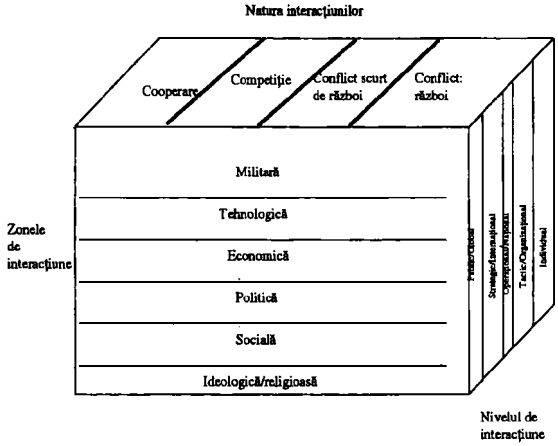


Figura 1. Domeniul Strategiei Războiului informaţional

Apărarea împotriva atacurilor informaţionale are câteva caracteristici în comun cu eforturile societăţii de a combate boala, drogurile şi crima. Notarea acestor similarităţi ne ajută să încadrăm problema, să oferim câteva lecţii utile şi să ne servim de o unitate de măsură.

Înainte de a trece în revistă câteva similarităţi dintre combaterea RI-D şi aceste probleme mai vechi, trebuie spus că, în timp ce eradicarea atacurilor informaţionale nu poate fi o aşteptare realistă, progrese semnificative pot fi făcute în apărarea contra tuturor tipurilor de atac, astfel că riscurile pot fi menţinute la nivelurile acceptabile. A ne apăra include posibilitatea de a preveni atacuri, de a face inofensive atacurile şi de a controla pagubele cauzate de acestea.

Problema RI-D este similară cu problemele întâlnite în eforturile de combatere a bolilor, drogurilor şi crimei. În primul rând, soluţionarea oricăreia dintre aceste probleme necesită eforturi din partea unui anumit număr de organizaţii publice şi private.

În al doilea rând, este puţin probabil, dată fiind competiţia pentru resurse, ca vreunul dintre aceste eforturi să fie sponsorizat în totalitate. De aceea, ne putem

aştepta să nu fie asigurat niciodată un nivel suficient de sponsorizare a programelor RI-D, aşa cum spun că ar trebui, cei care sunt responsabili cu problema RI-D.

În al treilea rând, acestea nu sunt probleme statice. Cartelurile de droguri şi criminalii cu siguranţă învaţă din greşelile lor. Chiar şi viruşii învaţă. De aceea, forţele de apărare sunt nevoite să ţină pasul cu atacanţii.

În al patrulea rând, conştientizarea şi implicarea publică vor atinge apogeul doar acompaniate de mari eforturi pentru soluţionarea problemei. Aceste scurte perioade de interes vor fi urmate de lungi perioade, în care graba de a soluţiona problema va face loc apatiei. A menţine sponsorizarea şi progresul, în perioadele de încercare de câştigare a interesului public, va fi una dintre principalele provocări din această zonă.

În al cincilea rând, organizaţiile şi indivizii vor învăţa să-şi ajusteze comportamentul pentru a trata problema atacurilor RI şi a consecinţelor lor nedorite.

În sfârşit, soluţiile vor presupune compromisuri. Acest lucru este datorat tensiunilor naturale care există între numeroşii deţinători de mize. Tensiunile dintre întărirea legii şi protecţia libertăţilor civile sunt câteva exemple clasice, care au apărut în domeniul informaţional.

Atacurile asupra sistemelor informaţionale sunt deja un fapt curent în viaţa de zi cu zi, în Epoca informaţiei. Deşi o mică parte din aceste atacuri au drept rezultat pierderi semnificative şi daune, marea majoritate produc pagube mici (care ar echivala cu infracţiuni cum ar fi: încălcarea proprietăţii private, vandalismul minor sau furturile mici).

A fost estimat că mai mult de 90% dintre aceste atacuri sunt comise folosindu-se mijloace şi tehnici disponibile marelui public (incidente raportate de CERT), că doar 1 din 20 de atacuri este observat de victimă, şi că doar 1 din 20 este raportat (aceste ultime două statistici sunt rezultatul studiului DISA [„Defensive Information Systems Agency”]. Cote similare au fost raportate şi de către alte instituţii). Cu toate acestea, se pare că

raportarea cotelor ar putea fi în creştere. Îngrijorătoare este prezenţa unei ameninţări „strategice” tehnice.

Mijloacele care există pot cauza daune serioase bunurilor informatice publice şi private, proceselor şi sistemelor informaţionale şi pot compromite integritatea informaţiei vitale. Analiştii n-au dificultăţi în identificarea grupurilor care au motivaţii şi oportunităţi pentru a lansa astfel de atacuri. Dată fiind vulnerabilitatea noastră, ca naţiune, un RI bine planificat şi coordonat poate avea consecinţe strategice.

Un astfel de atac, sau ameninţarea unui astfel de atac, poate veni în contradicţie cu obiectivele politicii noastre externe, poate degrada performanţa noastră militară, poate duce la pierderi economice semnificative şi chiar la subminarea încrederii cetăţenilor noştri în abilitatea guvernului de a-şi proteja cetăţenii şi interesele.

Chiar dacă până acum nu a existat vreun atac care să constituie o astfel de ameninţare, simpla existenţă a mijloacelor prin care se poate duce un astfel de atac, cuplată cu multitudinea motivelor şi oportunităţilor care există, reflectă starea noastră prezentă de vulnerabilitate. Aceste circumstanţe cer acţiuni defensive în interesul publicului. Trebuie să fim mai degrabă „proactivi”, decât să reacţionăm după o informaţie de tip „Pearl Harbour”. Din ce în ce mai des, un atac strategic reuşit va indica calea şi îi va încuraja pe alţii să plănuiască atacuri similare. De aceea trebuie să ripostăm întărindu-ne latura defensivă.

Fiecare epocă a văzut războiul transformat de tehnologiile şi conceptele acelui timp. Epoca informaţiei promite să nu fie diferită din acest punct de vedere, de predecesoarele sale. Unii au denumit războiul din Golf ca fiind primul „Război informaţional”, alţii l-au numit ultimul război din Epoca industrială. Puterea informaţiei a fost clar demonstrată în contextul conflictului tradiţional. Informaţia a îmbunătăţit efectiv eficienţa tuturor aspectelor războiului, de la logistică, la comandă, control, comunicaţii, şi computere, informaţii, supraveghere şi

recunoaştere (C4ISR).

Eficienţa SUA şi a aliaţilor săi, în războiul din Golf, a împiedicat cu siguranţă adversarii potenţiali de a răspunde forţelor noastre într-o manieră pe care Irakul a încercat-o şi a stimulat-o. Prin tehnologiile avansate şi prin globalizarea economiei, războiul digital oferă posibilitatea unei eficienţe mai mari, devenind astfel o strategie pe care adversarii potenţiali se gândesc să o adopte, pentru a îndeplini nişte obiective pentru care anterior se căuta o soluţionare prin mijloacele războiului tradiţional.

Război digital, un subset a ceea ce noi numim RI, implică atacuri care nu sunt fizice asupra informaţiei, proceselor informaţionale, şi infrastructurii informaţionale, care compromite, alterează, produce daune, întrerupe sau distruge informaţia şi/sau întârzie, aduce confuzie, înşeală şi blochează procesul informaţional şi decizional.

Războiul digital posedă câteva dintre caracteristicile pentru care factorii militari abilitaţi se luptau în trecut: precizie la un preţ scăzut, neparticipare şi secret.

Războiul militar ameninţă capacitatea armată a unei ţări de a se interpune între populaţie şi „duşmanii statului”, provocând astfel pierderea refugiului. Importanţa refugiului poate fi dedusă din dorinţa noastră de a cheltui importante resurse, în diferite domenii, pentru a asigura cetăţenilor noştri un refugiu funcţional în caz de pătrunderi teritoriale.

O altă caracteristică a atacurilor informaţionale provine din pierderea refugiului. Atacuri de acest gen, atunci când sunt mai mult decât un incident izolat, creează o percepţie a vulnerabilităţii, a pierderii controlului şi a încrederii în capacitatea unui stat de a asigura protecţie. Impactul poate să întreacă cu mult pagubele produse.

Această reacţie neliniară între daune reale şi daune sociale face ca problema războiului digital să fie o provocare specială, deoarece creează o nepotrivire între răspunsurile raţionale de apărare şi eficienţa lor.

Cum răspunde cineva la un set serios de atacuri informaţionale? A răspunde cu forţe militare tradiţionale

poate fi un fapt neacceptat politic sau poate fi ineficace. De cele mai multe ori, nu există un consens privind modul de a trata un astfel de atac, chiar şi printre persoanele din domeniul apărării, care sunt preocupate de aceste probleme.

Dată fiind potenţiala eficienţă a unui război digital ca instrument de putere pentru concurenţi şi pentru actorii nonstatali, noi, ca societate, trebuie să luăm în serios Epoca informaţiei şi noua sa formă de război. Dacă nu o vom face şi dacă ne vom baza doar pe arme şi concepte de război tradiţionale, vom ajunge să construim în secolul XXI propria noastră linie Maginot, care poate fi distrusă cu viteza luminii.

Există persoane care au sugerat că nu suntem, aşa cum s-a pretins, atât de vulnerabili la atacurile informaţionale, datorită faptului că sistemele noastre deţin un anumit potenţial de rezistenţă şi elasticitate. Acestea au scos în evidenţă suprapunerile existente la nivelul acestor sisteme şi consideră că ar fi foarte greu, pentru oricine, să distrugă complet un set dat de servicii.

Au arătat lipsa de interoperabilitate dintre sistemele moştenite, şi spun că ar fi imposibil pentru atacatori să ajungă foarte departe prin pătrunderea chiar şi a celor mai slabe sisteme şi folosirea lor drept căi de acces pentru a ataca alte sisteme. Ei spun că sistemele noastre şi interrelaţionările lor sunt dificil de înţeles chiar şi pentru noi, deci cu atât mai mult pentru potenţialii adversari.

Cu siguranţă este o doză mare de adevăr în fiecare argument. Dar această colecţie de puncte de vedere are dezavantajele sale. În ce priveşte consideraţiile asupra securităţii, cinci puncte trebuie subliniate.

În primul rând, important nu este faptul dacă un atac poate sau nu să distrugă în totalitate un sistem sau un tip de serviciu, ci dacă sunt suficiente daune pentru a atrage atenţia şi a provoca un comportament de panică, care poate crea la rândul său, o problemă semnificativă, de importanţă naţională.

În al doilea rând, redundanţele în sisteme sunt numai

parţiale şi neplanificate. De aceea ele nu sunt nici complete, nici de încredere.

În al treilea rând, sistemele noastre, multe fiind proiectate şi construite cu puţină sau chiar fără atenţie pentru securitate, sunt dificil de protejat şi de securizat.

În al patrulea rând, deoarece nevoile de interconexiune şi interoperabilitate cresc, din ce în ce mai multe sisteme sunt legate prin diverse „lucrări auxiliare”. Aceste poteci, compromit în multe cazuri, securitatea.

În final, lipsa de securitate produsă de aceste sisteme provoacă renunţarea la cererea de servicii, ceea ce face ca operaţiile să fie mai eficiente în multe domenii. Sistemele noastre uzuale au şi alte dezavantaje. De exemplu, lipsa interoperabilităţii duce la risipirea resurselor şi la diminuarea eficacităţii operaţiilor. Un lucru trebuie să fie clar: dezavantajele sistemelor noastre nu sunt o binecuvântare deghizată, ci mai degrabă sursa problemelor care trebuie să fie rezolvate, astfel încât noi să putem profita din plin de oportunităţile pe care tehnologiile informaţionale ni le procură.

Primul pas în abordarea oricărei probleme implică dezvoltarea unei *înţelegeri a mediului* („stări ale naturii”) cu care avem de-a face, a *opţiunilor pe* care le avem şi a *obiectivului care* este căutat. Acest lucru cere o identificare a variabilelor relevante, acelora care pot să influenţeze semnificativ rezultatul, dar şisubsetul acestor variabile relevante, care sunt controlabile, care formează baza pentru proiectarea operaţiunilor.

Într-o problemă atât de complexă ca RI-D, formularea problemei rezolvă trei aspecte. În primul rând, furnizează un schelet util pentru discuţie. În al doilea rând, serveşte să menţină atenţia focalizată pe acele arii specifice, care sunt fie necunoscute, fie în dispută. În al treilea rând, serveşte ca unitate de măsură pentru măsurarea progresului.

În acest caz, *mediul* corespunde naturii ameninţării cu care avem de-a face, vis-à-vis de vulnerabilităţile infrastructurii noastre informaţionale, în timp ce *opţiunile*

noastre corespund strategiilor pe care le adoptăm şi acţiunilor pe care le întreprindem pentru a ne apăra pe noi înşine. *Obiectivul* căutat corespunde nivelului performanţei infrastructurii, definirea şi măsurarea sa fiind o provocare însemnată prin ea însăşi şi a ei înşişi.

Un punct bun de pornire este încercarea de a dezvolta o înţelegere a naturii ameninţării sau mai precis a spectrului ameninţărilor relevante. Aceasta presupune o identificare a ameninţărilor potenţiale şi o estimare a probabilităţii lor. În mod normal, s-ar construi un set de stări ale naturii care sunt reciproc exclusive şi colectiv exhaustive, astfel încât o probabilă funcţie a densităţii să poată fi folosită. Stările naturii la care ne referim, corespund ameninţărilor potenţiale, grupate după un criteriu logic, menit să faciliteze analiza modului în care o strategie de apărare tratează fiecare din aceste ameninţări.

Având un concept iniţial al naturii şi şirul ameninţărilor potenţiale, cineva poate să dezvolte strategii de apărare alternative şi seturi de acţiuni corespunzătoare, pentru a le opune uneia sau mai multor ameninţări. Depinde mult, însă de ce variabile credem noi că putem sau că ar trebui să controlăm.

Fiecare strategie de apărare, cu setul său corespunzător de acţiuni, trebuie apoi să fie analizată în funcţie de fiecare ameninţare. Rezultatele acestor analize vor fi o caracterizare a rezultatelor sau a efectelor obţinute prin urmărirea fiecărei strategii de apărare care să ţină cont de fiecare ameninţare.

Aceste efecte, care sunt în principal descrieri ale rezultatelor (de exemplu: numărul penetrărilor şi consecinţele lor), trebuie apoi să fie traduse în măsuri de valoare, măsuri care reprezintă impactul lor. Costurile şi beneficiile asigura o bază raţională pentru realizarea unei strategii de apărare corespunzătoare. Datorită rolului central pe care tipologia ameninţărilor îl joacă în formularea problemei, ne vom întoarce atenţia acum, asupra examinării acestor categorii de ameninţări.

O înfăţişare grafică a topologiei ameninţării este prezentată în Figura 2. Natura neregulată a spaţiului indică faptul că graniţele sale nu sunt bine definite. Cu toate acestea, ameninţările se pot grupa după criteriul gravităţii consecinţelor lor (de la stânga la dreapta). Consecinţele asociate unui eşec merg de la consecinţe limitate şi izolate, la consecinţe de proporţii catastrofice.

Într-o serie de imagini, de la Figura 3 până la Figura 6, sunt înfăţişate diferite aspecte ale topologiei ameninţării. În Figura 3, spaţiul ameninţării este împărţit în trei zone. În partea din stânga a spaţiului putem să grupăm marea majoritate a ameninţărilor, a ameninţărilor de fiecare zi. Aceste ameninţări de fiecare zi (,,Everyday Threats"), au un anumit cost, însă nu ameninţă securitatea noastră naţională. În partea din dreapta a spectrului ameninţării este o mică suprafaţă care reprezintă acele ameninţări strategice care au implicaţii asupra securităţii naţionale. A treia zonă conţine ameninţări care pot avea implicaţii asupra securităţii naţionale. Aceste ameninţări potenţial strategice („Potentially Strategic Threats") reprezintă o provocare dificilă, aparte.

Există un număr relativ mic de ameninţări, cu care marea majoritate ar fi de acord că au implicaţii strategice (Figura 4), care trebuie apărate cu multă vigoare. Atacurile împotriva sistemelor care controlează armele de distrugere în masă („WMD") sau asupra reţelei noastre de comunicaţii urgente („MEECN") aparţin clar acestei categorii.

Alte ţinte strategice sunt sistemele de informare şi comunicare, asociate cu Autoritatea naţională de comandă („National Command Authority"), câteva dintre sistemele noastre de comandă, control, comunicare şi informaţii (C31) şi câteva dintre sistemele noastre de informaţii, mai ales informaţiile care privesc sursele şi metodele. În afară de aceste seturi de ameninţări, care aparţin clar fie categoriilor ameninţări de fiecare zi, fie categoriilor ameninţări strategice, sunt şi alte clase de ameninţări, care lărgesc spectrul ameninţărilor.

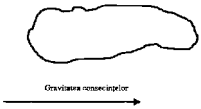
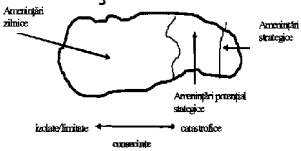


Figura 2. Spaţiul ameninţării

Atacurile asupra infrastructurii noastre naţionale (Figura 5) nu aparţin clar unei singure zone a tipologiei ameninţărilor, ci tuturor celor trei clase de ameninţări. Aceste atacuri, asupra siguranţei publice, sistemelor şi serviciilor de distribuire a energiei, asupra sistemelor şi serviciilor financiare şi de comunicaţii au implicaţii diferite şi consecinţe care depind de natura specifică şi de circumstanţele în care se desfăşoară atacul.



Rgura3. Tapés spaţiului ammiDţăni

Figura 4. Ameninţări strategice

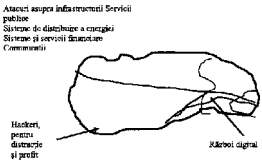


Figura S. Infrastructura ameninţărilor în timp ce unele dintre aceste atacuri pot avea consecinţe serioase, sub forma unor pierderi semnificative de date, servicii întrerupte sau bunuri şi servicii furate, numai un mic număr dintre aceste atacuri izolate poate avea consecinţe potenţial strategice.

Cu toate acestea, atacurile asupra infrastructurii pot fi serioase, dacă sunt bine planificate şi bine coordonate. Pentru aceasta este nevoie de un adversar cu un scop bine

definit, cu un sistem sofisticat şi cu o bună organizare. Acestui tip de atac i se potriveşte denumirea de război digital („Digital Warfare”). În funcţie de nivelul de sofisticare al unui atac, consecinţele acestuia pot ajunge până la consecinţe strategice.

Un punct important, care trebuie subliniat, este cel al naturii haotice a atacurilor asupra infrastructurii. Comportamentul haotic presupune o relaţie neliniară între input şi output, unde predicţia devine extrem de dificilă, dacă nu imposibilă. Două scenarii ilustrează această natura haotică.

În primul caz, un atac asupra infrastructurii poate să provoace o serie de consecinţe apropiate, dificil de prezis şi care măresc cu mult efectele atacului.

În al doilea caz, o serie de atacuri pot da dovadă de un comportament haotic atunci când suma consecinţelor lor nu poate fi determinată prin adăugarea consecinţelor lor individuale, sau când efectul lor cumulat întrece de departe suma efectelor individuale, a unei serii de întâmplări independente.

Aceste două scenarii nu sunt modele neobişnuite. Aceste modele se regăsesc şi în natură dând naştere unor discipline ştiinţifice, cum ar fi cele ale complexităţii, ale catastrofei, şi teoria complexităţii.

La fel stau lucrurile şi în privinţa atacurilor asupra ţintelor comerciale, reprezentate în Figura 6. În categoria ameninţărilor de zi cu zi intră atacuri care, în Epoca informaţiei, sunt o versiune a fraudei şi furtului – o continuare a crimei gulerelor albe şi o transformare a unei crime mai violente într-o formă care nu e fizica.

Aşa cum a arătat Dr. Horton (PDSAD (C31)), când unul dintre cei mai celebri hoţi de bănci a fost întrebat de ce jefuieşte bănci (dat fiind faptul că ele sunt aşa de bine apărate), acesta a remarcat: „acolo sunt banii”. Ei bine, „digital money” (bunurile şi serviciile) reprezintă banii în Epoca informaţiei.

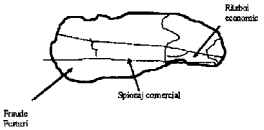


Figura 6. Ameninţări privind ţintele economice

Ca şi atacurile asupra infrastructurii, atacurile asupra ţintelor comerciale se pot manifesta în funcţie de circumstanţe, de la ameninţări de fiecare zi până la ameninţări strategice. Atacurile asupra ţintelor comerciale, realizate de către diferite organizaţii, nu vizează, de obicei, în mod direct banii, ci mai degrabă informaţii vitale (ex. secrete comerciale) şi au un mare potenţial de a provoca efecte mai serioase decât furturile izolate. Aceste atacuri, sub forma spionajului comercial, au consecinţe potenţial strategice, mai ales atunci când sunt vizate ramuri industriale cheie, de către companii străine.

Spionajul comercial se transformă în război economic, care ar putea să aibă consecinţe strategice, atunci când există eforturi dirijate de state, de organizaţii internaţionale, sau de alte grupuri străine.

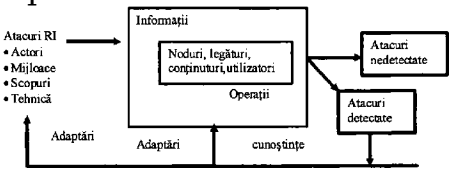
Aşa cum se poate vedea din seria de înfăţişări grafice ale tipologiei ameninţării prezentate mai sus, ameninţarea este multidimensională, într-un fel dezordonată chiar, şi se poate comporta într-o manieră haotică. Natura dinamică şi interactivă a ameninţării face apărarea împotriva atacurilor să fie mai dificilă.

Atacatorii şi apărătorii sunt prinşi într-o bătălie continuă a inteligenţelor şi resurselor (Figura 7). Din păcate, atacanţii posedă câteva avantaje. De exemplu, atacatorul poate să aleagă timpul, locul, mijloacele şi metoda de atac. Latura tehnologică este tot de partea atacatorului, deoarece este foarte dificil să dezvolţi apărări perfecte la un preţ pe care să ţi-l permiţi. De aceea, vor exista întotdeauna „găuri”.

Care dintre acestea vor fi exploatate rămâne o necunoscută până în momentul atacului. Din acest motiv, atacul este, de obicei, cu un pas înaintea apărării.

Atacatorii au, de asemenea, avantajul de a putea controla atacul, mult mai uşor decât ar putea s-o facă cei atacaţi.

Apărări



_ _ acumulate

Figura 7. Dinamic;

Orice întâmplare este un mediu de studiu pentru atacatori şi apărători – este un mediu dinamic. În acest mediu organic, atacatorii învaţă din atacurile nedetectate în momentul desfăşurării lor, indiferent dacă au fost reuşite sau nu. Atât atacatorii cât şi apărătorii se perfecţionează şi jocul continuă.

Acest aspect al ameninţării indică faptul că apărarea trebuie să constituie o preocupare continuă. De asemenea, sugerează faptul că strângerea şi analizarea informaţiilor despre atacuri este vitală pentru a putea ţine pasul cu atacatorii. În concluzie, apărătorii trebuie să fie activi şi să-şi asume eforturi care să conducă la o anticipare a metodelor atacului, astfel încât să poată fi dezvoltată o apărare eficace.

Problema privind eficacitatea unei apărări în faţa unei varietăţi de atacuri potenţiale este exacerbată de: incapacitatea noastră de a dezvolta o relaţie simplă, între un tip de atac sau ameninţare şi o organizare, de relaţia esenţială, neliniară, dintre rezultat şi valoare şi de faptul că variabilele-cheie nu sunt sub controlul nostru.

Descompunerea unei probleme ne ajută, uneori, să facem progrese, uşurând, cel puţin, stabilirea responsabilităţilor la nivelul instituţiilor. Aşa cum am văzut, problema RI-D rezistă descompunerii de-a lungul liniei organizaţionale. Aceasta se întâmplă deoarece există o slabă cartografiere a relaţiei dintre ameninţare şi organizare, din două puncte de vedere.

În primul rând, ţinta organizaţională a atacului este

foarte puţin legată de topologia ameninţării, deoarece atacul unei anumite Organizaţii, poate avea drept rezultat un set de consecinţe, care lărgesc spectrul ameninţărilor.

În al doilea rând, nu există o delimitare clară între responlàbilitatea organizaţională şi topologia ameninţării. Acest lucru este mai ales adevărat atunci când vorbim de suprafaţa identificată,ca fiind potenţial strategică.

Este întotdeauna mai uşor să rezolvi probleme cu funcţii obiective predictibile sau cu măsuri ale valorii. Aşa cum am văzut, tn RI-D există situaţii în care relaţiile dintre evenimente şi variabile se comportă într-o manieră haotică. Acest lucru introduce în ecuaţie o doză mare de incertitudine.

Dacă aceste două caracteristici ale problemei RI-D nu prezintă provocări semnificative, ne confruntăm totuşi cu faptul că unele dintre variabilele-cheie, care au influenţă asupra rezultatelor şi valorilor acestor rezultate, sunt numai parţial controlabile. De exemplu, fiecare dintre următoarele variabile, dacă este pe deplin controlabilă, ar putea fie să reducă semnificativ numărul sau severitatea atacurilor, fie să reducă impactul atacurilor: proliferarea tehnologiei, nivelul de conştientizare şi pregătire a personalului, disponibilitatea expertizei’pe computer, sistemul de apărare şi percepţiile publicului.

Am ajuns la sfârşitul discuţiei despre *natura* şi *caracteristicile* RI-D. În continuare este prezentat şi discutat un posibil mod de soluţionare a problemei.

Soluţia propusă în acest material este cea a unei strategii de „*apărare în adâncime*”, strategie care implică o succesiune de bariere defensive, din ce în ce mai puternice sau „mai înalte”, ce acţionează împreună, pentru a descompune spectrul ameninţărilor la componentele manageriale. În continuare, vom detalia această strategie a RI-D, natura separării responsabilităţilor, unele din condiţiile obligatorii pentru realizarea unui progres, provocărilecheie care apar, respectiv elementele unui plan de acţiune pentru organizaţiile cu responsabilităţi în domeniul RI-D.

Strategia de „apărare în adâncime” propusă, prezentată în Figura 8, constă în trei linii de apărare. Fiecare linie de apărare este proiectată în aşa fel încât să ia în considerare ameninţările asociate cu o anumită zonă a tipologiei ameninţării.

Prima linie de apărare este apărarea împotriva atacurilor zilnice, care constituie partea cea mai consistentă a tipologiei de ameninţare. Pe baza informaţiei disponibile, marea majoritate a acestor atacuri pot fi respinse cu apărări de bază.

Cele mai înalte niveluri de apărare, asociate atacurilor potenţial strategice sau strategice sunt responsabile cu împiedicarea celor mai sofisticate atacuri, care, însă, sunt şi cele mai rare.

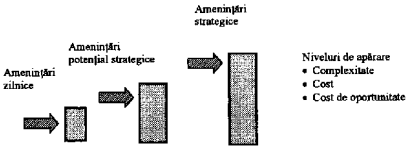
Abordarea apäi&iu & adfocime

Majoritatea atacurilor pot fi respinse cu apărări de bază

Niveluri mai înalte ale apărării sunt responsabile cu împiedicarea celor mai sofisticate atacuri, care sunt însă şi cele mai puţine, din mai puţine surse posibile

Fig. 8 Strategia de „apărare în adâncime”

Combinarea filosofiilor „mai întâi informaţia” şi „mai întâi securitatea”



De exemplu, atacurile cu implicaţii strategice ar trebui să treacă de primele două linii de apărare, care ar trebui să filtreze toate atacurile, exceptând doar adversarii cei mai pricepuţi, cei mai persistenţi, cu cele mai bune şi mai performante resurse. Acesta înseamnă că am putea să ne concentrăm eforturile asupra monitorizării unui segment mai redus al populaţiei, fapt ce va spori şansele de a obţine în apărare succesul scontat.

Strategia defensivă înseamnă, de asemenea, posibilitatea de a aplica diferite abordări filosofice fiecărei

linii de apărare, în funcţie de natura ameninţării. Cele două puncte de vedere ale spectrului filosofic pot fi acceptate ca abordări intitulate „mai întâi informaţia”, respectiv „mai întâi securitatea”.

În zona zilnică a tipologiei de ameninţare, abordarea noastră a pus accent pe accesul la informaţie. În zona strategică, se pune accent în primul rând pe securitate, prinrestrictionarea accesului şi a conexiunii.

Figura 9 reprezintă grafic o separare a responsabilităţii primare pentru RI-D, între sectorul public şi cel privat, ca o funcţie a tipologiei de ameninţare. Termenul „primar” este utilizat pentru a sublinia faptul că, atât instituţiile publice cât şi cele private au responsabilităţi în privinţa RI-D, chiar dacă acestea sunt asociate, într-un anumit domeniu, unuia din sectoarele public sau privat.

Zonele tipologice asociate ameninţărilor zilnice sau strategice sunt cele mai evidente. Responsabilitatea primară pentru ameninţarea zilnică ar trebui să revină sectorului privat. Rezolvarea acestei ameninţări reprezintă costul de a face afaceri în Era informaţiei. Presupunând costul relativ scăzut al apărării împotriva acestor tipuri de ameninţări, atribuirea acestei responsabilităţi sectorului privat devine posibilă. Mai mult, organizaţiile private sunt evident în cea mai bună poziţie pentru a înţelege propriile sisteme informaţionale şi nevoile şi preocupările clienţilor lor.

Răspunsul la ameninţările strategice este evident sarcina sectorului public, deşi o apărare adecvată va implica unele coordonări cu sectorul privat şi cu organizaţiile internaţionale, în special când apărarea este construită pentru a face faţă ameninţărilor asupra infrastructurii informaţionale naţionale sau asupra altor instituţii ce furnizează servicii vitale.

Răspunsul la ameninţarea strategică necesită acţiune guvernamentală coordonată cu sectorul privat şi cu grupuri internaţionale

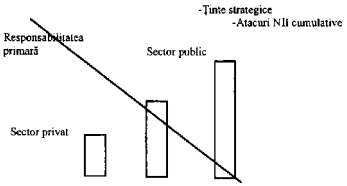


Figura 9. Separarea responsabilităţilor

Ameninţarea zilnică poate fi şi ar trebui să fie respinsă de fiecare instituţie -Costul de a face afaceri în era informaţiei -Există soluţii la cost scăzut pentru majoritatea ameninţărilor -Instituţiile sunt în cea mai bună postură pentru a înţelege sistemele /clienţii

Este mai puţin evidentă posibilitatea stabilirii responsabilităţii primare de apărare împotriva ameninţărilor din zonele potenţial strategice ale topologiei de ameninţare. Această zonă ar putea fi numită „zonă de colaborare”, unde este nevoie ca sectorul public şi cel privat să conlucreze pentru a înţelege ameninţarea şi pentru a dezvolta mecanisme eficiente care să ţină cont de ea.

Eforturile pentru a realiza o colaborare efectivă vor necesita depăşirea perspectivelor diferite de înţelegere ale instituţiilor. Instituţiile comerciale tradiţionale tratează atacurile zilnice ca un simplu cost necesar pentru a face afaceri, ce nu diferă semnificativ de un furt. Contramăsurile luate au o valoare aşteptată definită şi sunt angajate când costul lor efectiv este mai mic decât valoarea lor aşteptată.

Instituţiile tradiţionale din sectorul privat răspund la evenimente de probabilitate relativ redusă cu costuri posibil mai mari, rezultate din cumpărarea de asigurări sau obţinute prin furnizarea unei asigurări proprii.

Perspectiva securităţii informaţiei, oferită de instituţiile ce operează cu informaţii şi sisteme considerate vitale pentru securitatea noastră naţională, este destul de diferită. Spre deosebire de numeroasele atacuri informaţionale asupra sistemelelor din sectorul privat, costul unei breşe în securitatea unor informaţii de

importanţă naţională nu poate fi uşor determinat. Evidenţierea costului actual, al unui incident specific, este datorat faptului potrivit căruia protecţia sporită a integrităţii unor informaţii de securitate naţională şi a sistemelor ce le vehiculează are o valoare intrinsecă înglobată. Riscul evitării este răspunsul adoptat în aceste situaţii.

Potrivit naturii tipologiei de ameninţare a RI, securitatea informaţiilor din sectorul naţional şi sectorul privat sunt strâns legate. Atacurile asupra infrastructurii informaţionale globale sau naţionale pot afecta serios organizaţiile din sectorul privat. Acelaşi lucru se întâmplă şi în cazul atacurilor asupra instituţiilor-cheie din sectorul privat, ce pot furniza servicii vitale, atacuri care au implicaţii serioase în privinţa securităţii naţionale.

Aceste situaţii sunt conţinute în zona potenţial strategică a topologiei de ameninţare. Se propune ca în această zonă, spre deosebire de abordarea simplă „dolari şi cenţi", specifică zonei zilnice a tipologiei de ameninţare sau abordării prin evitarea riscului, specifică zonei strategice a tipologiei de ameninţare, să se adopte o abordare de management al riscului colectiv. Acesta este evident un domeniu care necesită ca apărările să fie coordonate îndeaproape.

Urmând firul logic a ceea ce am prezentat în legătură cu natura acestei probleme, ar trebui să fie evident pentru oricine că orice încercare de a realiza gestionarea RI-D într-o abordare centralizată este sortită eşecului. Dacă cineva are vreo îndoială, ar trebui să-şi reamintească de ameninţarea slabă existentă la cartografierea organizaţională, care previne rezolvarea efectivă a problemei cu „lanţuri de comandă pure" şi limitele posibilităţii Guvernului sau ale unei alte instituţii, de a controla variabile relevante.

Potrivit urgenţei şi importanţei acestei probleme este necesară o viziune pro-activă. Totuşi ar trebui să fie evident că o abordare de tip „laissez-faire" (rezolvare de la sine) este de asemenea sortită eşecului.

Este necesară o formă de orchestraţie (sincronizare) colectivă pentru a dezvolta gradul de conştientizare (luare în considerare) şi înţelegere a ameninţării pentru a dezvolta, în consecinţă, apărările necesare. Guvernul trebuie să stabilească ceea ce eu am HUmit „cadru pentru progres”.

Rolurile şi responsabilităţile specifice sectorului public şi privat vor fi diferite, în funcţie de tipul de ameninţări pe care leahi evidenţiat în scurta noastră trecere în revistă a fiecărei din pele trei zone importante ale tipologiei de ameninţare. În timp ce Iceastă discuţie s-a focalizat pe rolurile, responsabilităţile şi nevoia lie colaborare dintre structurile specifice SUA, problema RI-D a depăşit graniţele naţionale. Fără acorduri internaţionale specifice şi cooperare între naţiuni şi organizaţii internaţionale, posibilitatea noastră colectivă de a gestiona ameninţările va fi minimă.

Dezvoltarea celor şase domenii identificate în grafic vor netezi considerabil drumul nostru şi ne vor accelera progresul.

În primul rând, una din condiţiile obligatorii pentru progres este luarea în considerare a problemei şi a complexităţilor ei, precum şi generarea unui climat ce va facilita discuţia şi cooperarea între multe grupuri şi organizaţii, care trebuie să fie parte a acestui efort. Potrivit evenimentelor recente privind unele aspecte de securitate a informaţiilor, avem nevoie să începem reconstruirea legăturilor dintre unele grupuri şi organizaţii din sectorul public şi privat.

În al doilea rând, este important să ne desfăşurăm activitatea potrivit unei viziuni bine definite, care să evidenţieze clar ce încercăm să realizăm şi rolul corespunzător Guvernului.

În al treilea rând, „regulile jocului” trebuie dezvoltate şi promulgate. Multe din legile şi regulamentele noastre curente nu iau în considerare realităţile Erei informaţiei. Un set de reguli trebuie să se refere la stabilirea standardelor de securitate informaţională sau la un nivel

minim de apărare ce trebuie asociat cu diferite tipuri de date şi servicii informaţionale. Acestea vor fi similare cu recentele standarde private.

În al patrulea rând, interesul propriu, chiar lămurirea interesului propriu şi dorinţa indivizilor şi organizaţiilor de a fi buni cetăţeni, nu sunt suficiente pentru a ne asigura că vor fi dezvoltate şi angajate acţiunile şi apărările cele mai potrivite. Trebuie furnizate organizaţiilor guvernamentale resursele necesare pentru a ajuta la implementarea acestui cadru pentru progres şi la implementarea apărărilor necesare. E nevoie, de asemenea, să oferim stimulente care să încurajeze organizaţiile din sectorul public. În anumite cazuri particulare, Guvernul va fi nevoit chiar să furnizeze fonduri organizaţiilor din sectorul privat, pentru a pune la punct un sistem de securitate eficient.

În al cincilea rând, soluţia la această problemă depinde în mare măsură de cooperarea dintre organizaţii şi grupuri distincte. Este nevoie de dezvoltarea mecanismelor capabile să faciliteze şi să sporească cooperarea (incluzând stabilirea conţinutului colaborării, a grupurilor şi a locurilor special destinate).

În al şaselea rând, avem nevoie să stabilim responsabilitatea pentru numărul mare de sarcini pe care le implică un RI-D. Avem nevoie să decidem chestiuni de jurisdicţie. Avem nevoie să delimităm obligaţiile şi le facem cunoscute. În final, este necesar să stabilim clar responsabilitatea fiecărei organizaţii. Natura responsabilităţilor organizaţionale este discutată detaliat în continuare.

Niciunul din cele şase aspecte ale cadrului pentru progres nu încurajează ideea punerii în practică prea curând a acestuia. Considerând numai nevoia de revizuire a procesului legislativ, putem observa că va mai dura câtva timp înainte ca aceşti stâlpi de fundamentare să fie la locul lor. Totuşi e necesar să începem deja să purtăm o discuţie despre aceste elemente şi să încercăm să ţinem atenţia focalizată pe acest subiect.

Responsabilităţile organizaţiilor din sectorul public şi

privat diferă în funcţie de zona de ameninţare. În fiecare zonă de ameninţare, de la cea zilnică la cea strategică, fiecare sector al societăţii are unele responsabilităţi.

Responsabilităţi privind ameninţările zilnice.

Responsabilitatea primară pentru zona zilnică a tipologiei de ameninţare revine sectorului privat. În primul rând, organizaţiile din sectorul privat trebuie să-şi asume responsabilitatea pentru protecţia propriilor lor sisteme. Când legile şi regulamentele de securitate vor fi formulate şi adoptate, aceste organizaţii vor fi de asemenea responsabile pentru aderarea la aceste reguli ale jocului.

Dat fiind timpul necesar pentru dezvoltarea şi punerea în funcţiune a unui cadru legal şi regulamentar pentru operarea cu numărul mare de elemente ale securităţii informaţionale, se propune ca pe bază voluntară, organizaţiile din sectorul privat să-şi asume responsabilitatea pentru raportarea incidentelor. Este necesar să subliniem importanţa culegerii şi analizei de informaţii referitoare la atacurile informaţionale. Fără dezvoltarea unui ansamblu de cunoştinţe referitoare la aceste atacuri, eforturile pentru construirea apărărilor vor fi semnificativ îngreunate

Guvernul (incluzând nivelul federal, statal şi local) trebuie să-şi asume responsabilităţi certe pentru această regiune a tipologiei de ameninţare. În mod evident, Guvernul poartă responsabilitatea pentru protecţia sistemelor proprii şi pentru impunerea legilor şi regulamentelor corespunzătoare. Dată fiind importanţa realizării colaborării internaţionale în privinţa acestei probleme, ce nu cunoaşte graniţe statale, Guvernul trebuie să realizeze negocierea tratatelor şi acordurilor necesare.

Evident, culegerea datelor despre propriile sisteme este, de asemenea, responsabilitatea Guvernului. Dată fiind importanţa schimbului de informaţii, necesară obţinerii unei imagini precise a situaţiei, Guvernul trebuie să stabilească mecanisme pentru distribuirea, analiza datelor şi furnizarea rezultatelor. Vor trebui abordate elemente referitoare la clasificarea şi securitatea datelor.

Trebuie găsită o soluţie pentru a obţine informaţiile de care organizaţiile şi indivizii au nevoie pentru a se putea apăra ei înşişi.

Guvernul federal are responsabilitatea pentru apărare în zona strategică a tipologiei de ameninţare, utilizând suport din partea sectorului privat şi a guvernelor locale. Dată fiind dinamica şi natura interactivă a acestei situaţii, este important ca ameninţarea să fie înţeleasă cât mai bine. Cu toate acestea, utilizând informaţia culeasă precum şi informaţia raportată de alţii, Guvernul federal are responsabilitatea analizei strategice.

Guvernul federal are nevoie, de asemenea, să dezvolte o strategie de descurajare a potenţialilor atacatori. Sistemele strategice trebuie să fie monitorizate şi trebuie elaborate operaţii de supraveghere.

Evident, Guvernul federal are responsabilitatea protejării informaţiei strategice şi a sistemelor ce colectează, stochează, prelucrează şi transmit aceste informaţii.

În final, Guvernul federal trebuie să dezvolte planuri pentru reconstrucţia sistemelor avariate sau distruse şi a informaţiilor pierdute sau compromise, dar pentru elaborarea celor mai eficiente planuri ar trebui simulată o astfel de situaţie.

Sectorul privat are, de asemenea, un rol de jucat în această zonă a tiopologiei de ameninţare. Mai întâi, multe sisteme strategice depind, într-o anumită măsură, de disponibilitatea şi integritatea sistemului privat sau de informaţiile din sistemele guvernamentale de stat şi locale. În al doilea rând, unele sectoare private sau unele sisteme informaţionale guvernamentale locale şi de stat pot fi atât de importante încât au, indiferent de intenţiile şi scopurile atacatorilor, un caracter strategic. În cele două cazuri, organizaţiile trebuie să coopereze cu Guvernul federal pentru a proteja aceste sisteme informaţionale. Dezvoltarea unei înţelegeri adecvate a ameninţării necesită ca toate organizaţiile să raporteze incidente şi să partajeze datele referitoare la atacurile care au avut loc.

Astfel, altă responsabilitate ce trebuie să fie asumată de organizaţiile din sectorul privat este promptitudinea raportării incidentelor.

Separarea responsabilităţilor pentru această zonă a tipologiei de ameninţare nu este atât de uşor de realizat ca pentru celelalte două zone. În această zonă de colaborare, organizaţiile din sectorul public şi privat trebuie să găsească căi şi să creeze mecanisme ce generează o percepţie distribuită asupra naturii ameninţării, în particular asupra acelor aspecte ale situaţiei ce sporesc probabilitatea consecinţelor strategice. Suplimentar, ar trebui să fie găsite modalităţi pentru a întări apărarea noastră, prin posibilitatea de a diminua efectele atacurilor în această zonă şi chiar de a le împiedica să aibă consecinţe strategice.

În această zonă e necesar ca Guvernul să colaboreze pentru dezvoltarea înţelegerii ameninţării, în timp ce sectorul privat trebuie să sprijine eforturile Guvernului prin furnizarea datelor incidente. De asemenea, Guvernul trebuie să aibă iniţiativa în dezvoltarea coordonării mecanismelor proiectate, să sprijine atât îmbunătăţirea înţelegerii cât şi coordonarea apărărilor.

Cele două mari provocări asociate acestei zone de ameninţare sunt, mai întâi, identificarea începutului unui atac cu semnificaţie strategică, caracterizarea naturii şi scopului atacului şi în al doilea rând, efectuarea tranziţiei de la „starea de pace” la „starea de război”. Succesul proceselor şi mecanismelor dezvoltate prin coordonarea acestei tranziţii va fi important pentru succesul oricărei strategii a RI-D. Acest lucru include nu numai îmbunătăţirea tehnicilor şi instrumentelor de detectare, dar şi îmbunătăţirea posibilităţii de a stăpâni un atac, şi în felul acesta de a limita extinderea pagubelor şi consecinţelor sale. E nevoie ca Guvernul să asiste sectorul privat în aceste eforturi prin furnizarea resurselor şi suportului tehnic. Resursele pot lua forma unor taxe-stimulent (de încurajare) sau a unor plăţi directe, în cazul unor sisteme din sectorul privat considerate a fi de

importanţă strategică.

Pentru oricine care prosperă din provocări, apărarea împotriva RI este o zonă de muncă importantă. Există cinci provocări cheie cu care avem de-a face.

Prima provocare implică dezvoltarea unei mai bune înţelegeri a naturii şi caracteristicilor ameninţării, în societate şi între instituţiile acesteia. Succesul implică ca fiecare să fie familiarizat cu caracteristicile ameninţării. Totuşi este important ca noi să continuăm să muncim pentru a spori considerarea acestei probleme şi a dezvolta o mai bună înţelegere, atât a naturii ameninţării cât şi a vulnerabilităţii noastre.

A doua provocare o reprezintă dezvoltarea unei strategii de ripostă a atacurilor informaţionale digitale. Prima regulă a apărării este riposta. Nu este alocat suficient efort pentru dezvoltarea şi aplicarea strategiilor posibile. ACTIS a sponsorizat un atelier de lucru pe acest subiect. Acest atelier a fost un mare succes, oferindu-le participanţilor o mai bună idee despre cele mai recente reflecţii pe acest subiect, stimulând interesul pentru subiect şi aducând în atenţie unele elemente cheie (lucrările acestui atelier au fost publicate şi sunt disponibile prin intermediul ACTIS).

A treia şi a patra provocare implică dezvoltarea mijloacelor de furnizare a avertizării pentru atacuri şi modalităţi de apărare de succes. Îmbunătăţirea posibilităţii noastre de a identifica existenţa unui atac şi de a furniza indicaţii şi avertismente despre atacuri într-un anumită perioadă în timp, este poate cea mai dificilă provocare cu care avem de-a face.

Dezvoltarea unui mod de indicare şi avertisment presupune nu numai posibilităţi de atac tactic şi strategic, dar şi posibilitatea de a şti că un atac a început şi de a stabili, cu o anumită marjă de incertitudine, scopul acestuia. Ţinând cont de faptul că, în mod curent, un atac în desfăşurare nu este sesizat, această provocare capătă o semnificaţie importantă.

Nu este numai o provocare tehnică, ci şi una

organizaţională (aşa cum am menţionat mai devreme). Informaţiile necesare pentru a furniza avertizarea despre o acţiune iminentă şi un atac în stadiile lui timpurii este cel mai bine să vină din partea organizaţiilor sectorului privat, ale căror structuri de raportare ar trebui să pună la dispoziţie, într-un timp scurt, toate datele relevante.

Astfel, un atac de semnificaţie strategică poate să se fi încheiat înainte ca noi să realizăm existenţa lui şi să fim în măsură să trecem la „starea de război'4, lucru ce determină sporirea cerinţelor de raportare şi coordonarea necesară pentru a aprecia situaţia şi a răspunde corespunzător.

Ca rezultat al participării mele la o serie de jocuri de tip „după o zi*4 („day after") dezvoltate de RAND pentru ASD (C31), am ajuns la concluzia că nu vom fi în măsură să răspundem la timp, la astfel de atacuri, decât dacă există:

1) înţelegere şi luare în considerare a naturii posibilităţilor războiului strategic şi a propriilor noastre vulnerabilităţi, nu numai printre oficialităţile-cheie din organizaţiile publice şi private, dar şi din Congres, din cadrul mass-mediei şi a publicului;

2) o mai bună înţelegere a arsenalului ofensiv aflat la dispoziţia noastră, în special a efectelor directe, indirecte şi colaterale pe care acesta le poate cauza;

3) un sistem de preacord pentru alertă, similar cu sistemul DEFCON, ale cărui nivele susţin cunoaşterea şi înţelegerea proceselor şi acţiunilor practicate;

4) un proces de apreciere a pagubelor corespunzătoare RI.

Construirea unui sistem de tip DEFCON pentru RI-D va necesita investirea unei cantităţi considerabile de capital intelectual, precum şi o bună coordonare între Congres şi numărul mare de agenţii şi departamente guvernamentale, asociaţii industriale şi organizaţii private.

Opţiunile bine gândite, ce se adresează atât nevoii de culegere de informaţii şi de realizare a unei analize aprofundate, cât şi nevoii de a lua măsuri de prevenire sau de control al pagubelor, sunt esenţiale pentru considerarea

acestei ameninţări. Dată fiind topologia ameninţării, împărţită îh trei zone, şi natura foarte diferită a fiecăreia, implementarea strategiei de „apărare în adâncime” va fi o întreprindere considerabilă.

A cincia provocare se referă la dezvoltarea răspunsurilor corespunzătoare unor astfel de atacuri. Răspunsurile date acestor atacuri includ identificarea, interdicţia, previziunea şi pedepsirea (şi chiar răzbunarea).

Avem mult de învăţat şi pe mulţi de educat. Pentru a conştientiza ameninţările şi consecinţele unui RI nu este suficientă numai citirea romanelor sau mersul la filme. Când singurul contact cu subiectul este prin ficţiune nu este nicio mirare că ameninţarea poate fi tratată ca fiind ficţiune. Există încă mulţi indivizi ocupând poziţii-cheie atât în sectorul public cât şi în sectorul privat, care au nevoie să înţeleagă mai bine aceste probleme, pentru a fi mai motivaţi în abordarea fenomenelor.

Pe de altă parte, recunoaştem că nu posedăm o abundentă informaţie factuală.

Ignoranţa noastră în privinţa naturii atacurilor potenţiale este oglindită de lipsa de cunoştinţe despre eficacitatea tehnicilor şi strategiilor defensive dezvoltate în prezent.

Când sistemele noastre nu sunt monitorizate adecvat şi incidentele nu sunt înregistrate şi investigate corect, este greu de apreciat cum am putea dezvolta înţelegerea profundă atât a ameninţării cât şi a eficacităţii apărării necesare. Intensificarea culegerii de informaţii şi a analizei aplicate este necesară pentru a furniza fundamentarea empirică pentru:

a) sporirea conştientizării (luării în considerare);

b) sporirea înţelegerii noastre;

c) planificarea sprijinului;

d) dezvoltarea apărărilor efective.

Date fiind limitările pe care le avem impuse în cadrul unei colectări de informaţii interne, este puţin probabil că vor fi colectate şi analizate de către Guvern informaţii suficiente pentru a determina natura şi amploarea unui

atac informaţional, în stadiile lui timpurii.

Totuşi, este extrem de important ca atunci când un astfel de atac apare (este iminent sau în derulare) acea colecţie de date şi structurile de analiză din „timp de pace” să fie operaţionale şi în „starea de război”. În proiectarea unui echipament similar cu sistemul DEFCON, va fi importantă definirea evenimentelorindicator ce vor determina automat transmiterea informaţiei spre o structură de analiză a situaţiei.

Epoca armelor atomice a condiţionat perfecţionarea strategiilor de apărare şi de stăvilire a proliferării armelor nucleare. RI diferă de războiul atomic prin numeroase elemente, şi de aceea lecţiile învăţate din experienţă în privinţa realizării unei strategii ftincţionale de apărare, nu pot fi folosite în mod direct în problema apărării informaţionale, dar cu siguranţă pot asigura un punct de plccare pentru consideraţiile asupra RI-D.

Unele dintre problemele legate de dezvoltarea apărării împotriva atacurilor RI se referă la diferitele mijloace de ridicare a pragului atacului, folosind un RI ofensiv.

În timp ce ridicarea pragului de apărare este una din componentele specifice oricărei strategii de apărare, (făcând atacurile mai dificile şi mai costisitoare, limitând pagubele posibile), o nouă problemă se pune: ce înseamnă mai multă apărare?

Dat fiind costul mic necesar achiziţionării mijloacelor necesare purtării unui RI, actorii nonstatali pot constitui o ameninţare strategică. Cum se pot prevedea şi împiedica astfel de atacuri?

O altă problemă este cea a naturii acţiunilor care ar putea fi utilizate de către apărare şi relaţia dintre măsurile de contracarare şi cele de împiedicare a atacurilor informaţionale.

Abilitatea noastră de a apăra sistemele individuale şi informaţia utilizată este fundamentul oricărei strategii şi abordări a RI. Pentru a atinge un nivel performant de apărare, trebuie:

1) să revizuim abordarea noastră asupra proiectării şi achiziţiei unui sistem;

2) să înţelegem dimensiunile apărării;

3) să întreţinem dezvoltarea unor tehnologii cheie.

Tendinţa actuală în proiectarea sistemelor este de a asigura un accès lărgit, pentru un număr tot mai mare de informaţii, la toate nivelele organizaţionale. Noua noastră abordare a sistemelor de informaţie implică un „reach back", ce presupune că indivizii nu „împing" informaţia, ci mai degrabă „scot" informaţia cerută, din diversele baze de date. Dirijaţi de ciclul scurt de viaţă al tehnologiei informaţionale şi de bugetele micşorate, devenim din ce în ce mai dependenţi de software. Acest lucru face din ce în ce mai greu de asigurat integritatea informaţiei.

Dacă trebuie să construim nivelul apărărilor contra atacurilor RI, trebuie să asigurăm utilizatorii cu nivelul de siguranţă cerut, pentru a le da încredere în sistemele lor. De aceea avem nevoie de câteva schimbări în abordarea noastră în privinţa proiectării sistemului şi achiziţiei. Din mai multe motive, unul dintre ele fiind securitatea, trebuie să ne concentrăm mai mult pe asigurarea informaţiei de calitate, aceasta însemnând să modificăm continuu relaţia „date – informaţie – înţelegere – cunoaştere".

În evaluarea proiectelor de sistem şi în stabilirea standardelor pentru sistem, trebuie să creştem setul curent de măsuri de merit („MOMs") pentru informaţie. Faţă de atribute ca timpul şi acurateţea, trebuie să ne concentrăm în plus pe autenticitate, integritate şi valabilitate.

Conexiunea este importantă pentru a atinge nivelurile de funcţionalitate dorite, dar o subliniere accentuată a interoperabilităţii securizate este necesară pentru a realiza obiectivele RI defensiv.

„Operaţiile şi menţinerea activităţilor" („O&M") asigură oportunităţi pentru a preveni intruziuni şi pentru a întări apărările sistemului. Operatorii de sistem şi de menţinere a software-ului sunt adesea cei mai puţin experimentaţi. Dată fiind natura critică a O&M pentru

menţinerea sistemelor de apărare, practicile O&M trcbuiesc revizuite.

Apărarea este o funcţie mai mare decât proiectarea şi asigurarea calităţii software-ului. Are multe dimensiuni, unele dintre ele fiind ilustrate în Figura 10. Fiecare dintre aceste dimensiuni trebuie considerată în funcţie de fiecare sistem şi set de circumstanţe.

În plus faţă de modul de proiectare a unui sistem, aceste dimensiuni ale apărării includ operaţii de sistem, metode şi proceduri folosite pentru a limita atractivitatea şi/sau consecinţele unui atac. Figura 10 prezintă câteva dintre dimensiunile apărării care trebuie să fie luate în considerare în construcţia unui sistem de apărare informaţional.

Fiecare dimensiune oferă un set de alegeri care asigură mai multă sau mai puţină protecţie. Mai multă protecţie tnseamnă un anumit preţ (surprinzător, preţul poate fi mic, mai nies dacă îl comparăm cu câştigurile în securitate pe care le putem obţine).

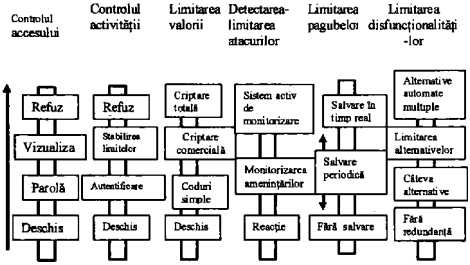


Figura 10. Dimensiunea apărării

Construcţia apărărilor presupune existenţa mijloacelor pentru realizarea acestora. Multe dintre capacităţile de apărare, pe care le avem în mod obişnuit, nu sunt adecvate pentru anumite nivele cunoscute sau tipuri de atac. Acestea sunt domenii unde am putea folosi progresele în tehnologie.

Timpul real de detectare a intruziunii este în mod cert un clement-cheie, în orice set de apărări. Capacitatea noastră de a detecta, în timp real, incursiunile în sistemele noastre şi identitatea agresorului, este limitată. Nu-ţi ia

mult timp pentru a susţine un atac informaţional. Daune pot apărea în orice clipă. Este clar că ar fi de dorit o capacitate automată de a răspunde la o intruziune, çare să poată preveni sau limita pagubele.

Dată fiind creşterea confidenţei noastre pe COTS trebuie să gflsim căi pentru cost – eficienţă, pentru a fi siguri că software-ul pe care l-am cumpărat face ceea ce vrem noi şi numai ceea ce vrem noi. Orice instituţie din Epoca informaţiei cumpără milioane de linii de cod în fiecare an, ale căror origini exacte nu sunt cotate cu niciun grad de încredere. Existenţa unor instrumente automate pentru a realiza încrederea de calitate şi pentru a verifica şi valida codul, ar fi de mare ajutor.

A şti cu precizie că datele nu au fost alterate sau compromise şl că sursa unei baze de date a fost verificată, ar ajuta muh în efortul nostru de a combate atacurile informaţionale.

Piatra de încercare a eforturilor noastre de a combate RI va fi efortul tuturor organizaţiilor de a-şi proteja propriile sisteme şi Informaţia. Unele organizaţii s-au îngrijit de acest lucru de mai mult timp şi au dezvoltat şi implementat planuri de a se menţine hl lop, faţă de creşterea serioasă a setului de ameninţări. Alte organizaţii mai au încă multă muncă de depus în acest domeniu.

Ar putea fi folositoare, chiar şi acelor organizaţii care simt că sunt bine pregătite, revizuirea următoarei liste de acţiuni, pentru a determina toca ce trebuie făcut, pentru a fi mai bine pregătite pe viitor.

Prima acţiune sugerată implică o revizuire a misiunii organizaţiei în lumina noilor ameninţări. Anumite organizaţii vor observa că RI-D adaugă o nouă misiune sau creşte importanţa misiunii existente.

Cine este responsabil cu RI-D în organizaţie? Poate că organizaţia are un Ofiţer Şef de Informaţie şi ar fi indicat ca acesta să-şi asume responsabilitatea. Poate că responsabilitatea RI-D este partajată de mai mulţi indivizi. În orice caz, este necesară o alocare clară a responsabilităţilor.

Nu toate informaţiile sau toate sistemele ar trebui considerate egale în ceea ce priveşte protecţia. Este important, date fiind constrângerile de resurse, să identificăm care informaţie şi care sisteme (şi funcţii ale acestor sisteme) sunt critice şi care nu.

Cât de vulnerabile sunt informaţiile şi sistemele? Care este natura specifică a vulnerabilităţilor? Răspunsurile sunt necesare pentru a asigura o bază de date pentru a planifica şi dezvolta apărările. Trebuie reţinut că natura vulnerabilităţilor evoluează constant. Aşadar, analizele vulnerabilităţilor trebuie să facă parte dintr-un efort continuu.

Acţiuni izolate pentru a îmbunătăţi securitatea sunt de ajutor, dar ele nu sunt substitutul pentru dezvoltarea comprehensivă a strategiei RI defensiv pentru organizaţie. Din moment ce nu este posibil să evităm toate riscurile asociate cu RI, fiecare organizaţie trebuie să elaboreze un plan de administrare a acestor riscuri.

În cursul dezvoltării şi articulării unei strategii organizaţionale şi a planului de management a riscului în RI defensiv, multe probleme vor fi discutate. Aceste discuţii vor crea o mai mare conştientizare a problemei în cadrul organizaţiei şi va îmbunătăţi abilitatea organizaţională de a face faţă provocărilor asociate cu RI defensiv.

A combate RI este o problemă care trebuie privită pe termen lung. Strategiile de investiţie ale unei instituţii trebuie revizuite. Unele realocări de resurse pot fi necesare datorită schimbărilor survenite în costurile operaţionale şi datorită introducerii de noi proceduri şi măsuri de protecţie.

CONCLUZII

Problema apărării împotriva atacurilor informaţionale este reală. Cetăţenii noştri şi organizaţiile care le asigură servicii vitale sunt foarte expuşi acestui fenomen. Costul scăzut al acestor atacuri a lărgit câmpul adversarilor potenţiali şi a complicat eforturile de a strânge informaţii şi de a se apăra. Consecinţele unui atac

bine planificat şi coordonat pot fi serioase. Rămâne de văzut cum va răspunde publicul unei ameninţări de atac asupra infrastructurii.

Această situaţie se accentuează odată cu proliferarea rapidă a tehnologiei informaţionale şi a competenţei în domeniu. Devenim tot mai dependenţi de sistemele automate, în fiecare aspect al vieţii noastre.

Deoarece tehnologia informaţională devine o parte importantă a modului în care organizaţiile şi indivizii creează, produc şi asigură servicii, nevoia de interconexiune şi interoperabilitate între acestea creşte. Odată cu nevoia crescândă de schimburi de informaţiii (şi produse), cresc şi vulnerabilităţile.

Dată fiind situaţia actuală, trebuie să ne concentrăm, în principal, asupra a două lucruri. În primul rând trebuie să găsim o modalitate de a ne proteja pe noi înşine de atacurile informaţionale şi în al doilea rând, trebuie să elaborăm un fundament stabil, care să ne permită să facem progrese sigure, ridicând continuu costul unui atac şi limitând paguba aşteptată.

OPERAŢIILE INFORMAŢIONALE. CÂTEVA REFLECŢII OPERAŢIONALE SISTEMUL SISTEMELOR

JMJ BOSCH[10]

Operaţiile informaţionale pot fi înţelese doar în contextul mai larg al schimbării şi continuităţii. „Ciberspaţiul” este asemenea pământului, apei, aerului şi spaţiului, o dimensiune în care războiul poate fi dus, unde apărarea este o necesitate, în timp ce atacul este o posibilitate. Există o legătură strânsa între „războiul bazat pe informaţie” şi „operaţiile informaţionale”.

Operaţiile informaţionale n-au impact numai asupra domeniului militar, ele pot de asemenea produce efecte şi la nivel naţional, internaţional şi chiar global, influenţând astfel un stat, o alianţă de state sau chiar opinia publică internaţională. În cele din urmă la toate nivelele este nevoie de comandă şi control pentru a menţine ordinea în sistem. Fără a minimaliza importanţa tehnologiei, în cele

10 Academia Militară Regală, Breda, Olanda.

din urmă omul este cel care decide şi care acţionează.

Dată fiind dependenţa noastră de tehnologia informaţională şi de comunicaţie (ICT) şi de opţiunile de a manipula informaţia, ne confruntăm azi cu noi ameninţări; provocarea este aici şi acum. Frustrarea este o consecinţă a complexităţii schimbării.

Există o listă aproape fără sfârşit de cărţi, articole şi alte publicaţii despre informaţie ca mijloc, ţintă sau armă, pe scurt despre „războiul bazat pe informaţie" şi despre „operaţiile informaţionale".

În al doilea rând, se poate observa complexitatea varietăţii de schimbări care influenţează deja sau vor influenţa în curând comanda şi controlul. Scopul articolului este, în esenţă, unul de natură militară. În primul rând, tratează perspectiva observatorului militar, care încearcă să înţeleagă prezentul şi viitorul, care se confruntă cu schimbări ale vitezei procesării moderne computerizate. Să ne gândim la soluţii este singurul lucru care ne rămâne de făcut, pentru a putea înţelege provocarea. Ţelul meu este să descriu înţelesul şi implicaţiile războiului bazat pe informaţii şi operaţii informaţionale pentru a sensibiliza conştiinţele [11].

Unii ar putea să susţină că trăim într-o eră a prea multor schimbări. O dată cu dispariţia confruntării est-vest, stabilitatea s-a diminuat şi a dat naştere mai multor schimbări. Actuala scenă internaţională are sute, dacă nu chiar mii de actori care se luptă pentru putere, influenţă, bani şi atenţie.

Statele se număra şi ele printre aceşti actori. În această arenă complexă, dezvoltările economice, ecologice, demografice, culturale şi tehnologice pot conduce, singure sau în combinaţie, la conflict. Bogăţia este destul de inegal răspândită dacă comparăm estul cu vestul şi nordul cu sudul. Există o puternică legătură între creşterea economică şi cea demografică.

---

11 Primele idei în acest sens au fost introduse de autor în lucrarea „operaţiile informaţionale. Schimbare sau frustrare?", publicată în DSEi ('oiifereiîce Proceedings (1999), vol.2, p. 3-10.

Schimbări în mai bine survin doar atunci când creşterea economică depăşeşte în mod substanţial creşterea populaţiei. A treia dimensiune este ecologia. Ne confruntăm şi aici cu o distribuţie inegală de materiale şi energie. Apa este o adevărată problemă deoarece nu există niciun fel de substitut pentru această problemă.

Cultura, a patra dimensiune, merită şi ea atenţie. Acolo unde graniţa săraci-bogaţi coincide cu graniţa culturală, şi acolo unde identitatea este în pericol, percepţia şi convingenle religioase pot genera forţe cu o dinamică periculoasă. Mijloacele de informare în masă sunt atât spectatori cât şi comentatori. Ele sunt uneori strict controlate.

Fiind un pod între „mesaj" şi auditoriu, ele influenţează sentimentele colective, emoţiile şi pot forţa decizii, inclusiv în ce priveşte folosirea forţei. Apoi, mai există ştiinţa şi tehnologia pe temelia cărora orice societate îşi construieşte capacităţile sale de a produce bunuri şi servicii – inclusiv de natură militară –, de a organiza şi de acţiona.

Tehnologia informaţională şi de comunicaţii (ICT), combinaţia de computere şi de telecomunicaţii, afectează toate aspectele de fiecare zi ale vieţii, societatea şi lumea în care trăim. Biotehnologia este un domeniu promiţător atât pentru medicină cât şi pentru agricultură sau pentru arme noi.

Tehnologia spaţială poate duce la noi opţiuni pentru comunicaţii, supraveghere şi management al mediului înconjurător care poate afecta toate celelalte domenii. Încă din 1998, Centrul de Cercetare Ames, de la NASA, din California, a prezentat un concept pentru un sistem revoluţionar de transmisii construit din atomi şi molecule. Acest sistem constituie în sine o revoluţie: „nanonizarea" maşinilor şi sistemelor. Dar cum tehnologia înseamnă putere şi bani, ea este o sursă potenţială de conflict.

Ea se adaugă la sursele de conflict existente, ca răspândirea inegală a populaţiei, spaţiul de locuit, bogăţia şi apa. O ultimă sursă este chiar istoria în sine, deoarece a

lăsat neîncheiate socoteli şi a adus – cel puţin unora – ură şi supărare. Date fiind aceste observaţii, definiţiile şi conceptele tradiţionale de securitate sunt tot mai inadecvate.

Cea mai mare provocare a zilelor noastre este să înţelegem lumea complexă în care trăim şi tendinţele care se prefigurează pentru viitor. Foarte probabil, vor fi tendinţe viitoare diferite în funcţie de cine suntem şi unde trăim. După Van Creveld, trăim în „epoca automatizării", după soţii Toffler, suntem parte a celui de-al „treilea val", trăim în „epoca informaţională". Atât schimbarea cât şi continuitatea însoţesc omenirea. Constantele sunt lupta pentru putere, influenţă, bogăţie şi nevoia continuă de adaptare la o schimbare fără de sfârşit.

Au lost şi vor fi dezbateri interminabile despre revoluţiile tehnologice militare. După unii autori, noi o experimentăm acum pe a zecea. Alţii folosesc criteriul cronologic pentru a ilustra schimbările revoluţionare. Dupuy a descris, folosind drept criteriu viteza şi procesul schimbărilor tehnologice, patru perioade [12]. Slipchenko, un general maior rus, a afirmat că războiul din Golf a prezentat o parte din cele şase generaţii de arme[13]. Van Creveld a descris patru epoci: „epoca uneltelor", „epoca maşinilor", „epoca sistemelor" şi cea de-a patra, începând de prin 1945, „epoca automatizării".

După soţii Toffler, noi ne aflăm acum în „cel de-al treilea val". O nouă tehnosferă, o nouă sferă a informaţiei, o nouă sferă industrială, instituţii noi şi noi tipuri de război în care informaţia are o valoare critică, marchează acest val, ce-şi are originile în SUA, în perioada 1955 şi 1965.

Există o vastă discuţie despre numere, motive, efecte şi sens al revoluţiilor. În schimb, nu se discută prea mult despre faptul că ele se produc acolo unde se întâlneşte viziunea cu tehnologia în noi concepte, organizări şi moduri de operare. În cele din urmă, toate schimbările au fost efectul unei combinaţii de factori.

12 Dupuy, volumul 6, p. 2702.

13 Bowdish, p. 26 şi notele de final 4-6.

Impactul revoluţiilor vine odată cu definiţia, este decisiv întrun anumit moment în istorie. Pe termen lung – cu excepţia armelor nucleare – revoluţiile tind să fie pietre de hotar în procesul de evoluţie. Statele, şi prin ele armatele, au obţinut mijloace mai sofisticate pentru a le utiliza în conflict.

Cuvântul „revoluţie” are un înţeles special. În general, pot fi observate patru tendinţe. Prima are de-a face cu depăşirea limitărilor fizice şi psihice ale fiinţei umane, a doua cu creşterea vitezei, distanţei, preciziei şi letalităţii armelor. A treia se ocupă de protecţie. A patra se îngrijeşte de păstrarea controlului şi comenzii, în ciuda armelor noi disponibile, a mediului, a oponentului, a elementului de surpriză.

Soldatul individual tinde să devină, ceea ce corporaţia RAND numea, „Cavalerul Jedi”; cu un simţ supradezvoltat, indestructibil, invizibil şi letal. Vom asista la sisteme de senzori, mai mari sau mai mici, care vor folosi unde micro din spectrul radio şi fuziuni de date. Ne vom putea aştepta la arme cu energie, precum laserele şi armele electromagnetice. Vom vedea arme non-letale noi, mai bune şi va exista un spectru de posibilităţi mai larg pentru a ataca omul, maşina sau softul.

Metodele merită şi ele o atenţie specială. Unii ar putea găsi noi căi de a utiliza „vechi” metode precum războiul biologic, chimic şi ecologic, războiul de guérilla, şi, aşa cum se va arăta pe parcursul acestui articol, războiul informaţional. În cele din urmă, schimbarea în cadrul sectorului militar este întotdeauna legată de tehnologie. Dar războiul şi conflictul sunt marcate de numeroase constante.

Ele sunt marcate de voinţe, deprinderi şi ucideri. Comanda şi controlul are întotdeauna de-a face cu incertitudinea şi trebuie să găsească căi pentru a evita fricţiunea, „această teribilă fricţiune”, aşa cum arăta Von Clausewitz. Fricţiunea este mai mult decât efectul fricii, al exhaustivităţii şi incertitudinii despre „ei” şi „noi”.

Ea are de-a face de asemenea cu norocul, coincidenţa

şi ghinionul. Fricţiunea azi este mult mai complicată decât a fost altădată. Clausewitz nu trebuia să se gândească la război aerian, spaţial, la războiul de coaliţie sau la presă, etc.

În schimb, forţele moderne trebuie să se gândească la toate aceste lucruri. În cele din urmă, mai intervine şi elementul surpriză. Esenţa comenzii nu este să reduci fricţiunea, ci să învingi toate provocările. Ultima constantă este nevoia continuă de adaptare la o schimbare continuă. Constantele sunt într-adevăr legate de om.

În timpul primului război mondial, armatele au ajuns să înţeleagă sensul unei a treia dimensiuni. Al doilea război mondial a tăcut loc celei de-a patra dimensiuni, dimensiunea electronică, alături de care s-a stabilit şi dimensiunea psihologică. Tot atunci au început să se lege primele idei despre folosirea spaţiului. Noţiuni de genul „ciberspaţiu”, „sferă informaţională” sau „lume digitalizată” fac ca operaţiile informaţionale să devină o adevărată problemă.

Al doilea război mondial a acţionat ca un catalizator pentru multe dezvoltări: război mecanizat, operaţii combinate, război în apă, sub apă şi în aer. Rezultatul a fost introducerea radarului, sisteme noi de comunicare, rachete şi computere. Idei timpurii precum cele ale lui Charles Babbage (1792-1871) s-au materializat îti concepte precum „motoare de diferenţiere” şi, în 1834, „motoare analitice”.

Hollerith a creat echipamentul de calcul în 1890. În 1939, Atanasoff, un matematician şi fizician american, a construit ceea ce unii numesc primul prototip al unui computer electromecanic digital. În 1944 a văzut lumina zilei calculatorul automat cu secvenţă controlată, Harvard Mark I, care a dus în 1946 la realizarea computerului digital complet electronic, cunoscut sub acronimul de ENIAC.

Pentru mai mult timp, un alt Mark I a fost puţin cunoscut; el a fost dezvoltat la Bletchley, şi a fost prevăzut pentru acţiuni împotriva Enigmei, sistemul german de

criptare. În 1943, a fost introdus primul Colossus, care utiliza 15000 de tuburi electronice; trei luni mai târziu a apărut Colossus II, cel care i-a dat lui Hollerith ideea unei noi dimensiuni[14].

În ambele armate, atât în cele din Vest cât şi în cele din Est, computerul s-a dezvoltat dintr-un lucru rar, uneori chiar secret în ccea ce este el astăzi. Însă dezvoltarea lui nu face obiectul studiului de faţă. Computerele sau chiar mai bine tehnologia informaţională sunt acum „un fapt normal de viaţă”. În acelaşi timp, este relevant să observăm că aceste computere sunt maşini.

Oricine ştie că inputuri proaste dau naştere la outputuri pe măsură. Toată himea ar trebui să ştie că nu există program soft fără erori. După Welsh, un program militar standard poate număra 2% fisuri [15]. Aşadar nu există o fundamentare reală pentru o încredere absolută în ceea ce un computer „spune”. Ba chiar mai mult. În 1998, o companie germană a dezvoltat un soft care transforma – prin Internet – orice computer personal fatr-un instrument de spionaj. Tehnologia informaţională şi de comunicaţii influenţează armatele moderne, societăţile şi lumea în general.

Armatele moderne nu pot opera fără aşa numita „sferă informaţională”. Complexitatea crescândă a organizaţiilor ca rezultat al diversităţii sistemelor de arme de înaltă precizie şi cu rază lungă de acţiune şi creşterea continuă a vitezei, nevoia de intelligence, de coordonare şi de sincronizare în combinaţie cu factorul timp au dat naştere la ceea ce numim noi azi lumea digitală.

Forţele armate sunt administrate, comandate şi controlate prin intermediul tehnologiei informaţionale şi a comunicării. Tehnologia informaţională şi comunicaţiile sunt mai mult dec&t o combinaţie de tehnologie computerizată, micro şi nano tehnologie, fuziuni de date şi inteligenţă artificială. Aplicarea lor în cadrul sistemului de comandă şi combinarea lor stau la baza digitizării

14 Lewin, p. 129-133.

15 Welsh, p. 29.

câmpului de luptă.

Apoi există naţiuni modeme. Prin intermediul tehnologiei informaţionale şi de comunicaţii, naţiunile modeme organizează guvernul, realizează aprovizionarea cu apă şi energie, asigură transportul, reglementează serviciul bancar, finanţele, comerţul ş.a.

Tehnologia informaţională şi comunicaţiile conectează mijloacele de informare în masă cu public diferit. Toate acestea sunt conectate printr-o formă care poartă numele de „infrastructura informaţională naţională (NII)". În cele din urmă există, o infrastructură informaţională internaţională, chiar globală (GII), care conectează producători şi pieţe, bănci şi finanţe, guverne şi alte organizaţii, şi bineînţeles mijloacele de informare în masă şi auditoriul, precum şi indivizii.

Intemetul cu sutele sale de milioane de utilizatori este doar un element din această infrastructură. Naţiunile sunt doar una dintre categorii printre multele instituţii şi alti actori care aparţin acestor sfere supranaţionale. Tehnologia modernă face posibilă lărgirea rapidă a mediului.

O mică invazie a reporterilor de televiziune, radio, a oficialilor guvernamentali şi non-guvernamentali împreună cu mijloacele lor de comunicare conectează pur şi simplu acel mediu la o infrastructură informaţională la distanţă. Această combinaţie de infrastructuri informaţionale militare, naţionale, internaţionale, globale şi mediul creează acel ceva ce poate fi numit „ciberspaţiu44

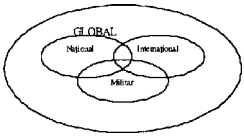


Figura 1: *Informaţia despre mediul înconjurător* în cadrul acestui spaţiu, se poate duce război la fel ca şi pe pământ, pe mare, în aer sau în spaţiu, având drept instrument de acţiune directă, comanda şi controlul. Suntem martorii unei noi dimensiuni de război: dimensiunea electronică şi psihologică au început să

păleasică. În cadrul acestui ciberspaţiu, operaţiile informaţionale au dejucat un rol crucial.

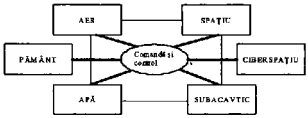


Figura 2: Dimensiunile războiului înainte de a începe analiza conflictului în această dimensiune câteva remarci asupra războiului bazat pe informaţie se impun.

În conformitate cu „Joint Vision 2010”, forţele armate care folosesc „sistemul sistemelor” vor câştiga cunoaşterea spaţiului de luptă şi vor putea răspunde la timp. În conformitate cu TRADOC Pamphlet 52505, toate activităţile vor produce în cele din urmă o »forţă totală”, capabilă să conducă un război terestru.

Această forţă va avea cinci caracteristici: flexibilitate doctrinară, mobilitate strategică, adaptare şi modularitate, conectivitate integrată, multinaţională şi conectivitate interagenţială şi versatilitate.

Sistemul de comandă se bazează pe noi căi de a folosi tehnologia informaţională şi de comunicaţii. Comandanţii vor avea o imagine comună, relevantă a bătăliei. Concentrarea se realizează pe spectrul supremaţiei. Combinând aceste dezvoltări cu concepte de operaţii în adâncime şi atac simultan se creează un mod dinamic de a extinde bătălia în spaţiu, timp; de reducere, dacă nu ciliar eliminare, a timpului şi nevoii de modulare a câmpului de luptă. Acesta este mesajul[16].

Dar dezvoltările merg chiar şi mai departe. În anul 2025 ar trebui să existe ceva de genul „Internet viu”. După Perricelli, ar Irebui ca fiecare individ de pe câmpul de luptă să poată interacţiona în orice moment, în timp aproape real. Această aşa numită „Sferă informaţională „ asigură transport informaţional şi servicii informaţionale luptătorilor, independent de localizare, grad de mobilitate

16J 8 Pentru mai multe detalii a se vedea Morris J., Boyd şi Michael Woodgerd.

sau dinamică platformelor [17].

Ecranele computerelor şi băncile de date nu dau imaginea în totalitate. Unele aspecte precum motivarea, estimările, sentimentele, personalitatea şi cultura sunt greu de depozitat sau de vizualizat. Dacă vorbim despre oameni implicaţi într-un război real, este recomandabil să citim „Military Misfortunes” de Eliot A. Cohen şi Richard Gooch. Mulţi militari uită să traducă experienţele în acţiune.

Apoi, există fluxul şi folosirea informaţiei. Doar datele şi informaţiile nu pot susţine deciziile. Iar şi iar, omul va trebui să selecteze, să analizeze, să interpreteze şi să evalueze pentru a putea decide şi acţiona. Se poate astfel ajunge şi la forme de „patologie informaţională”.

Prăpastia între ceea ce putem şti şi ceea ce putem cunoaşte 80 adânceşte. Abilitatea de a produce informaţie a crescut; abilitatea de a procesa informaţie nu s-a îmbunătăţit. Fluxul lıţplimentar de informaţie induce sentimentul de „fără putere”.

Într-un experiment, 1313 manageri din mai multe ţări şi-au exprimat părerea asupra informaţiei.: 49% erau adesea neputincioşi să digere informaţia valabilă; 65% se aşteptau ca viitorul să aducă mai puţin stres[18].

O maşină este logică, „omul” este logic doar uneori. Omul diferă în multe privinţe de o maşină. În termeni logici, el (sau ea) Ctfte inferior. Nu este surprinzător că în cele din urmă computerele reuşesc să-i bată la şah pe marii jucători. Unele acţiuni şi contraacţiuni în război pot fi definite în termeni logici: o rachetă ce vine, dirijată prin radar în combinaţie cu o armă defensivă.

Dar multe acţiuni într-un război sunt în afara acestui tărâm, în acest context, omul este cel mai preţios dar şi cel mai limitat factor. Cel mai preţios pentru că creativitatea şi sentimentele contează atunci când este vorba de un conflict. Limitat, pentru că omul depinde de caracterul său, de informaţii, de mediul înconjurător şi de experienţă.

17 Perricelli, Robert F. P. 34-39.

18 „Dying for information", Executive Summary

Comandantul are de-a face cu un set complex organizaţional, fizic, interpersonal şi psihologic, care este controlat de cerinţe şi reguli ale misiunii, de climă şi oboseală, de relaţiile de comandă şi de afinităţi cu tovarăşii de lupta, de ambiţie şi de frică.

SISTEMUL SISTEMELOR. În primul rând, el dă o viziune comună a câmpului de luptă. A vedea acelaşi lucru pe ecranul unui computer, nu înseamnă a împărtăşi aceeaşi interpretare. Imaginea mediului inconjurător este colorată de ceea ce ştim, de ceea ce nu ştim, de ceea ce credem că ştim şi de ceea ce credem că nu ştim, dar, de asemenea, şi de caracterul şi cunoştinţele celor care împart ecranul şi de circumstanţele cu care ei se confruntă.

În al doilea rând, viteza. Cum putem combina acţiuni la diferite nivele, atât pe orizontală cât şi pe verticală, astfel încât viteza să fie sincronizată? O diferenţă în viteză poate conduce la pierderea momentului, la luarea de decizii pripite sau chiar în sens larg, la punerea în pericol a comenzii şi controlului.

În al treilea rând, comanda şi controlul. Situaţia de avertizare a tuturor poate fi în acelaşi timp şi o binecuvântare şi un blestem. Pe de-o parte, pot să existe neînţelegeri asupra persoanei care trebuie să decidă, asupra a ceea ce trebuie să decidă, asupra celui care stabileşte prioritătile şi dă ordinele.

Pe de altă parte, există riscul micro-managementului. Sincronizarea este cheia acţiunilor integrate. Nu numai procesul este cel care contează – organizarea acţiunii în termeni de spaţiu şi timp – dar şi efectul, rezultatul pe care-l dorim. Nu există acţiune integrată Iară coordonare şi sincronizare; realităţile spaţiului de luptă pot uneori să necesite iniţiativă şi răspuns imediat.

În al patrulea rând, celelalte efecte. Într-o unitate pe deplin digitizată nu există hărţi reale, cu greu se găsesc instrucţiuni sau ordine scrise. Acest lucru înseamnă că viteza într-o „asemenea unitate depinde de cel mai puţin digitizat element.

Dacă sistemul eşuează, comanda şi controlul pot ajunge într-un punct mort deoarece totul se bazează pe informaţie computerizată fără nicio alternativă. Harta militară cu o gaură în interiorul ei este totuşi o hartă, pe când dintr-un computer în care s-a tras un glonţ nu mai rămâne nimic. Există trei tipuri de asimetrie tehnologică: Prima este atunci când partenerii dintr-o coaliţie se bazează diferit pe tehnologie. A doua se manifestă atunci când partenerii se bazează în egală măsură pe complexul tehnologic dar utilizează forme diferite. A treia variantă apare atunci când partenerii, care se bazează în egală măsură pe tehnologie similară, o folosesc în diferite scopuri.

În al cincilea rând, pot oamenii să se încreadă în sisteme şi în informaţiile pe care acestea le produc? Aşa cum s-a arătat şi mai înainte, omul nu este computer şi este supus distorsionărilor datorită emoţiilor şi motivaţiilor. El poate de asemenea să fie victima manipulării. Cum se poate preveni degradarea semnificativă sau, chiar mai rău, manipularea? Cum se poate „ataca" un adversar? Cum se poate opera în cadrul mediilor informaţionale înrudite? Răspunsul la aceste întrebări poate fi găsit în cadrul complexului modern de realităţi a comenzii şi controlului.

În literatura de specialitate, aşa numita „OODA-loop" (Observare, Orientare, Decizie şi Acţiune) este adesea folosită pentru a ilustra procesul şi ciclul de comandă şi control (C2).

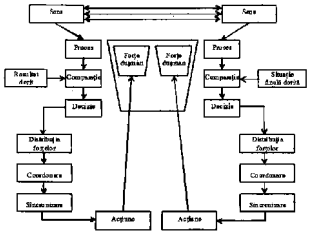


Figura 3: Cele două cicluri de comandă-control opuse în realitate, o organizaţie militară în acţiune este o maşinărie complexă unde sute, chiar mii de celule la diferite nivele de organizare – fiecare având propria viteza

– trebuie să fie coordonate şi sincronizate. Viteza fiecărei celule este influenţată de calitatea proprie, de aranjamentele organizaţionale, de tehnologia disponibilă, de complexitatea problemelor care trebuie rezolvate şi de circumstanţe.

Coordonarea cu un singur element se poate realiza într-un timp foarte scurt. Dar coordonarea şi sincronizarea mai multor celule presupune o altă dimensiune. În cele din urmă, şi poate cea mai importantă consideraţie: OODA-loop a fost introdus pentru a rezolva o problemă; C2 are alt scop. Figura 3 prezintă o ilustrare realistă a procesului şi ciclului de C2 în cea mai simpla situaţie: cea a doi comandanţi care se opun [19].

Dar chiar şi această ilustrare este o simplificare. Nu acordă prea mare importanţă faptului că există mai multe cicluri la diferite nivele. De asemenea neglijează faptul că mulţi se preocupă în acelaşi timp cu protejarea şi susţinea forţelor, cu treburile administrative, precum şi cu planurile acţiunilor viitoare. Ambele cicluri au ca scop să susţină acţiunea şi să influenţeze sau să neutralizeze oponentul. Finalitatea comenzii este menţinerea controlului. Acest lucru reprezintă mai mult decât a susţinut Van Crefeld, „reducerea incertitudinii”[20]. Criterii pentru un sistem perfect de C2:

Păstrarea ordinii şi coeziunii ropriilor forţe;

Controlul spaţiului de luptă şi evitarea ciocnirilor fatale;

Optimizarea alocaţiilor, strategiilor sau compoziţiei forţelor [21].

COMPLEXUL DE COMANDĂ ŞI CONTROL (C2C) O

generalizare acceptabilă pentru ceea ce înseamnă

---

19 Lawson a pus bazele în 1977. Hughes a introdus combinaţia celor două cicluri: cea aliată şi cea duşmană (Hughes, p, 187). Autorul a introdus distribuţia forţei, coordonarea şi sincronizarea ca elemente esenţiale.

20 Van Crefeld, p. 235-249.

21 Hughes, p. 191 referindu-se la Welch aşa cum este citat în Hwang la p. 4-6.

„informaţie” poate fi exprimată astfel: „cea care reduce incertitudinea” M, cu alte cuvinte, date atent selecţionate, organizate, relevante şi – ori de câte ori este posibil – la timp.

Sistemul informaţional funcţionează precum venele şi nervii unui complex mai larg de comandă şi control. Procesul de comandă şi control traduce date şi informaţii în ordine. Într-un sens mai restrâns, orice sistem informaţional modern are şapte componente de bază; „senzori, procesori, receptori, date şi informaţii, baze de date, transmiţători şi reguli”. În esenţă, comanda şi controlul sunt Sprijinite de către un sistem C2. Complexul de comandă şi control (C2C) cuprinde totul: factori de decizie, hardware şi software, Infrastructură.

Tabelul 1 arătă într-o manieră ce separă, elementele celor două părţi opuse:

Apărare proprie	Atac
Senzori, procesori, receptori, baze de date, transmiţători	Senzori, procesori, receptori, baze de date, transmiţători.
Infrastructură, putere, transport	Infrastructură, putere, transport
Date, informaţii, software, reguli	Date, informaţii, software, reguli
Comandanţi, consilieri şi alţi sustinători ai sistemului	Comandanţi, consilieri şi alţi sustinători ai sistemului
Trăgători, alţi actori şi utilizatori	Trăgători, alţi actori şi utilizatori

Informaţia a fost din totdeauna importantă; chiar în Biblie putem citi că spionii au fost folosiţi în recunoaşterea terenului şi observarea inamicului. C2 a fost din totdeauna o ţintă. Calul Troian este un bun exemplu de inducere în eroare de timpuriu. O dată cu dezvoltarea conceptului de C2, noi opţiuni de atac au fost găsite. Această înţelegere a condus la apariţia conceptului de război de comandă şi control (C2W).

În cadrul NATO, războiul de comandă şi control este definit ca *„ folosirea integrată a distrugerii fizice, a războiului electronic, inducerii în eroare, operaţiilor psihologice şi de securitate, sprijinite de către intelligence pentru a interzice adversarului accesul la propriile informaţii, influenţarea, degradarea, confuzia sau chiar distrugerea capacităţilor de C2 ale adversarului şi pentru protejarea partenerilor împotriva unor astfel de acţiuni*”[22].

Obiectivele măsurilor de război de comandă şi control constau în deschiderea, menţinerea sau chiar lărgirea diferenţelor de eficienţă a C2-ului în favoarea foiţelor aliate. Războiul de comandă şi control ofensiv este eficient, mai ales în domeniul economic pentru reducerea luptei adversarului. Este aplicabil la toate nivelele de comandă. Obiectivele primare ale războiului de comandă şi control împotriva potenţialului de luptă al unui duşman constau în:

Încetinirea tempoului operaţiilor sale;

Întreruperea operaţiilor sale;

Degradarea ciclului C2 de comandă al duşmanului;

Distrugerea abilităţii sale de a genera putere de luptă;

Scăderea dorinţei sale de luptă.

Prezervarea sistemelor prietene de C2 – războiul de comandă şi control defensiv – este o consideraţie fundamentală, deoarece eşecul este foarte probabil să conducă la pierderea libertăţii de acţiune şi iniţiativei, la o redirecţionare a efortului sau chiar la eşecul operaţiei. Obiectivele primare ale războiului de comandă şi control defensiv constau în:

Reducerea vulnerabilităţilor elementelor de C2 pentru atac;

Reducerea efectelor operaţiilor de securitate inamice împotriva sistemelor C2 prietene;

Neutralizarea efectelor acţiunilor de război electronic împotriva sistemelor prietene de C2;

Împiedicarea inamicului de a exploata sistemele C2

22 ATP 35 (B), capitolul 2. A se vedea de asemenea MC-348.

prietene;

Ineficientizarea acţiunilor psihologice inamice.

Deşi războiul de comandă şi control indică „prezervarea sistemelor de C2 prietene”, este clar că adevărata sa preocupare este „comanda şi controlul” în întregul său.

Distrugerea fizică nu mai are nevoie de precizări suplimentare.

Războiul electronic include efortul de a câştiga intelligence prin observarea şi evaluarea folosirii de către duşman a spectrului electromagnetic [23]. Inducerea în eroare constă îû manipularea duşmanului, distorsiunea, falsificarea evidenţei pentru a-i sugera să reacţioneze într-o manieră contrară intereselor sale.

Scopul de bază al inducerii în eroare ofensive este de a obţine suipriza şi de a menţine iniţiativa. Scopul de bază al măsurilor defensive este sa îmbunătăţească securitatea şi să stabilească condiţiile pentru operaţiile viitoare [24]. Inducerea în eroare trebuie direcţionată spre o ţinta umană, care este de regulă comandantul inamic şi staff-ul său şi se bazează pe reacţiile lor posibile.

Operaţiile psihologice au trei scopuri: să slăbească dorinţa adversarului, să câştige sprijinul celor nehotărâţi, să întărească loialitatea celor care sunt deja adepţi declaraţi. Operaţiile psihologice trebuie coordonate cu informarea publică, cu activităţile civile.

Nu există o definiţie universal acceptată pentru conceptul de „operaţii informaţionale”. Americanii în documentul FM 100-6, din iunie 1996, defineau operaţiile informaţionale astfel:

Operaţii militare permanente în cadrul MIE (*Military Information Environment*) *care dau posibilitatea, întăresc şi protejează abilitatea forţei aliate de a culege, procesa şi acţiona asupra informaţiei pentru a obţine avantaj faţă de toate categoriile de operaţii militare*; *Operaţiile militare presupun interacţiunea cu GIE* (*Global*

23 P.2-35.

24 P.2-36.

în formation Environment) *şi exploatarea capacităţilor adversarului de informare şi decizie sau chiar sabotarea procesului acestuia, de luare a deciziilor prin împiedicarea accesului său la informaţii*.

Departamentul american al apărării a venit şi el cu o definiţie a operaţiilor informaţionale: *acţiuni întreprinse pentru a afecta informaţia adversarului şi sistemele informaţionale în timp ce sunt apărate informaţiile şi sistemele proprii*.

Cea mai recentă definiţie (publică) americană se găseşte în doctrina USAF: *Operaţiile informaţionale sunt potrivite pentru orice tip de acţiune militară, atât pe timp de pace cât şi pe perioada unui conflict. Forţele aeriene sunt convinse că pentru înţelegerea deplină şi achiziţia superiorităţii informaţionale, înţelegerea noastră asupra operaţiilor informaţionale trebuie să includă doi piloni conceptuali distincţi dar care interrelaţionează unul cu celălalt*: *informaţia în război – aspectele de „câştig" şi „exploatare" sau alte procese ce se bazează pe informaţie – şi războiul informaţional – aspectele care se referă la „atac" şi „apărare"*.

Războiul informaţional (*RI*) *este alcătuit din operaţii Informaţionale conduse pentru apărarea propriilor informaţii şi*

S

isteme informaţionale sau pentru atacarea şi afectarea Bformaţiilor şi sistemelor informaţionale ale adversarului. Hspectul de apărare este operativ tot timpul.

În schimb, aspectul ofensiv se manifestă în primul rând pe Itoip de criză sau conflict. Războiul informaţional presupune Activităţi diverse precum operaţiile psihologice, inducerea în ètoare, războiul electronic, atacul atât ßzic cât şi informaţional (*ciberratacul*) *şi o întreagă gamă de activităţi şi programe defensive. Este important de subliniat faptul că războiul Informaţional este o construcţie care operează atât pe timp de pace cât şi de război, pentru a permite executarea efectivă a*

responsabilităţilor Forţei Aeriene [25].

Reflectând asupra acestor definiţii trebuie să subliniem faptul că ele într-adevăr diferă. Cu toate acestea, ele au un element comun: informaţia şi sistemele informaţionale. Toate definiţiile se axează pe realizarea superiorităţii informaţionale. Prin superioritate informaţională se înţelege *„capacitatea de a culege, procesa şi disemina un flux continuu de informaţii în timp ce este exploatată sau chiar interzisă abilitatea adversarului de a face acelaşi lucru. „* [26]

Informaţia seamănă mai degrabă cu un bun. Ea capată înţeles dacă éste folosită în acţiune. Informaţia poate conduce la înţelegere şi la introspecţie. Aceasta din urmă, împreună cu înţelesul, timpul şi spaţiul, ar putea să creeze şi să păstreze libertatea de acţiune şi să realizeze comanda şi controlul efectiv. „Ultra” (sistemul german de decodificare a semnalelor) şi „Magic” (sistemul japonez de decodificare) din al doilea război mondial, n-au făcut propriu-zis nimic, nu au ucis pe nimeni, n-au scufundat niciun vas şi n-au doborât niciun avion.

Pentru aceste lucruri au fost necesare oameni şi maşini. Dacă cineva acceptă că există ceva ce poate fi numit „ciberspaţiu”, atunci conceptul de „ciber-superioritate” nu poate fi decât acceptat, cu toate că are o natură abstractă şi are un înţeles doar în combinaţie cu alte elemente precum semnificaţie, timp şi loc. Care este adevăratul înţeles al superiorităţii informaţionale?

În cele din urmă înţelegerea, cel de-al şaptelea simţ este cel care contează. Jucătorii de şah au toate informaţiile la îndemână şi cu toate acestea pot să nu înţeleagă ce presupune o anumită mişcare. Războiul este mult mai complicat decât şahul. În lumea conflictului există mai multe dimensiuni, una dintre părţi deţine mijloacele de a influenţa una sau mai multe dimensiuni şi există reguli, unele ce decurg din limitările tehnologice, altele ce ţin de legea războaielor, de consideraţii etice.

25 AFDD 2-5.

26 Blinker, p, 13, nota de subsol 31.

Dar aceste reguli nu fac legea. Ele pot sau nu să limiteze o serie aproape fără de sfârşit de opţiuni. Că să-l citam pe Holcomb, operaţiile militare „nu sunt mecanice, iar comanda şi controlul reprezintă mai mult decât pur şi simplu urmărirea de proceduri stabilite sau culegerea a cât mai multor informaţii”.

Ipotezele digitizării armatei (dacă, în cadrul unei forţe digitizate, diferite tehnologii şi doctrine sunt integrate, aşa cum trebuie, în cadrul forţelor, atunci creşteri în letalitate, şanse de supravieţuire şi ritm vor fi câştigate) se pot baza pe falsa presupunere că operaţiile militare sunt mecanice. Ele sunt – aşa cum indica şi Clausewitz – descrise ca contracarând fricţiunea.

De aceea, întregul concept de digitizare poate fi o conceptualizare simplistă. Însă, aici trebuie făcută o diferenţiere între diverse forţe. Până la un anumit nivel, operaţiile aeriene şi maritime pot fi descrise ca mecaniciste. Platformele, armele şi sistemele lor pot fi descrise în termeni de viteză, înălţime, acurateţe. Dar numărul „actorilor”, interacţiunea cu elementele adverse, care pot folosi inducerea în eroare sau să acţioneze într-o manieră imprevizibilă şi interacţiunea complexă dintre om, maşină, vreme, teren, pune anumite limite predicţiei.

Simulările pe computer nu pot să stăpânească gândirea şi »creativitatea comandanţilor; deciziile lor sunt greu de replicat. Atunci există riscul să credem că având destulă informaţie şi comunicaţii bune, putem, aşa cum spune Holcomb: „să precizăm ţotul despre duşmanul nostru, iar ceea ce mai rămâne este doar o ftncţionare eficientă a sistemului pe care noi îl controlăm”.

În aceste condiţii este doar o chestiune de timp până în momentul în care duşmanul se va recunoaşte înfrânt. După părerea ţa, tscopul C2 nu este dominarea informaţională, ci crearea, alcătuirea şi distribuirea puterii de luptă, în timp ce este acceptată ideea că incertitudine există întotdeauna. Digitizarea nu trebuie ifi fie niciodată un scop în sine.

Mai există încă o consideraţie. Ce s-ar fi întâmplat

dacă în timpul primului război mondial, celui de-al doilea război mondial, forţele ar fi cunoscut toate detaliile? Cunoaşterea poate fi un înlesnitor, dar cu siguranţă poate fi şi o povară.

Şi o altă chestiune. Să presupunem că ştim dar suntem împiedicaţi să ne folosim cunoaşterea din cauza inducerii în eroare, a secretului sau a altor implicaţii. Limitate la domeniul militar, operaţiile informaţionale includ toate elementele de C2W. Dar acestora li se mai adaugă noi opţiuni: folosirea de arme HERF şi de bombe EMP. Apoi mai sunt viruşii şi alte mijloace de manipulare a informaţiei. Pregătirile şi operaţiile militare nu se materializează într-un vacuum.

Această legătură cu mediul înconjurător justifică denumirea de „război în reţea" („netwaie"). Acest război doreşte să,*jtntrerupă*, *să modifice ceea ce populaţia ţintă ştie sau crede că ştie despre ea însăşi şi despre lumea înconjurătoare* în literatura de specialitate, acest concept de influenţare a factorilor de decizie, fie direct, fie indirect, prin intermediul publicului larg, mai poartă şi numele de „război de percepţie" sau „război neocoitical". De fapt, el este strâns legat de arta propagandei. Vechi concepte şi noi instrumente se întâlnesc, pentru a manipula adevărul Chiar şi în ziua de azi, nu există nici-o garanţie că o anumită imagine reflectă realitatea, că anumite cuvinte au fost rostite întradevăr. Adevăratele ţinte rămân în continuare factorii de decizie.

Strategii ruşi susţin: *„Războiul informaţional este o cale de rezolvare a unui conflict dintre două părţi. Scopul este ca una dintre părţi să câştige şi să păstreze avantajul informaţional asupra celeilalte. Acest hicm poate fi realizat, prin exercitarea unei influenţe informaţionale/psihologice şi tehnice, specifice, prin sistemele naţionale de luare a deciziei, prin intermediul populaţiei, prin structurile informaţionale, ca şiprin înfrângerea sistemului de control al duşmanului, a structurilor sale informaţionale cu ajutorul unor mijloace*

suplimentare, precum armele, materialele nucleare. „[27]

Operaţiile informaţionale mai pot avea şi altă dimensiune. Aşa cum indica şi Harcknett acest gen de operaţii pot fi folosite pentru „întreruperea sau distrugerea legăturilor cu societatea, prin ţinte precum transportul, comunicarea, energia şi instituţiile financiare”[28].

Corporaţia RAND scrie despre „*folosirea ciberspaţiului pentru afectarea operaţiilor militare strategice şi pentru aducerea de prejudicii infrastructurilor informaţionale naţionale*”[29]. Un astfel de atac asupra societăţii poate avea consecinţe foarte grave. Nu este nevoie de prea multă imaginaţie pentru a înţelege ce înseamnă, de pildă, oprirea aprovizionării cu energie pentru societatea modernă.

Tabelul 2 oferă câteva exemple de elemente vitale pentru asigurarea comenzii şi controlului în cadrul Statelor Unite.

Culpepper Switch – se ocupă de toate transferurile electronice ale fondurilor federale;

Electronic Switching System (ESS) – administrează tehnologia Internet;

Time Distribution System – de care depind toate reţelele de calculatoare;

Global Positioning System – GPS;

World Wide Military Command and Control System (WWMCCS);

Principalele legături de satelit (Suitland, Bölling);

Federal Reserve Computing System;

Submarine Communication Center;

Reţeaua de televiziune y în acest context, nu este deloc surprinzător faptul că multe ţfai studiază aceste riscuri potenţiale. Întrebarea care se pune acum: există sau nu o contradicţie în a avea atât conceptul de război de comandă-control cât şi conceptul de operaţii informaţionale?

---

27 Grau şi Thomas, p. 508.

28 Harcknett, p. 95-96.

29 Molander, Riddle şi Wilson, p. 84 şi nota de subsol 1.

Pâna la un anumit punct, răspunsul poate fi da; ambele concepte se concentrează pe comandă-control, ca pe ceva ce poate fi atacat sau apărat. Există însă şi câteva argumente care au contribuit la noul concept, acéla de operaţii informaţionale. Primul este legat de dependenţa crescândă a organizaţiilor militare de tehnologia informaţională şi de comunicaţii.

O mare parte din calitatea finală a complexului de comandăcontrol depinde de calitatea datelor, de receptarea lor în timp oportun, de software şi de legislaţii. Există acum noi mijlolace de manipulare şi de distrugere a acestor facilităţi. Conceptul prezent de C2W nu ia în calcul ceva de genul unui atac de software. Al doilea argument ar fi cel legat de faptul că operaţiile informaţionale nu se limitează doar la vremuri de criză sau conflict. Acţiuni asupra sistemelor de comandă-control şi asupra informaţiei au loc acum.

Mai multe ţări au raportat activităţi ale hackerilor, crackerilor şi activităţi controlate, probabil, de grupuri sau state, cu intenţia de a pătrunde în sisteme, de a descoperi parole şi de a accesa informaţia. Interconexiunea cu diferite medii informaţionale creează vulnerabilităţi, care pot fi exploatate în orice moment. Ţinta poate fi societatea sau chiar comunitatea internaţională, aşa cum se arăta şi în figura 4.

Al treilea argument se leagă de constatarea că nu mai există graniţe clare între noţiunile de prieten şi duşman. Realitatea politică complexă aduce în prim plan oponenţi, susţinători ascunşi, aliaţi în diferite forme, neutri. Această realitate înlesneşte folosirea cu succes a războiului psihologic şi a propagandei chiar şi în afara unui conflict armat. Acest lucru forţează naţiunile să-şi reconsidere poziţia lor faţă de mass-media sau de folosirea sau nefolosirea informaţiilor. Un alt argument este legat de conceptele de coordonare şi sincronizare. Conceptul de C2W necesită „folosirea integrată a cinci acţiuni militare principale: distrugerea fizică, războiul electronic, inducerea în eroare, operaţiile psihologice şi

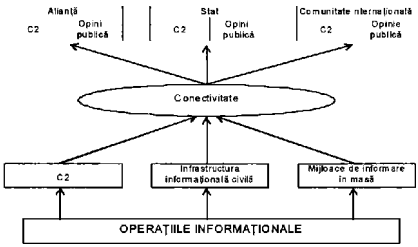


Figura 4: *Scopul operaţiilor informaţionale*

OPSEC. De asemenea, acest concept mai subliniază şi importanţa coordonării operaţiilor psihologice cu informaţia publică, treburile civile şi activităţile CIMIC. În lumea în care trăim, orchestrarea cere o concentrare clară, un nou concept şi noi linii directoare. Bosnia Herţegovina şi conflictul din Cecenia sunt lecţii din care trebuie să învăţăm.

Războiul din fosta Iugoslavie este un bun exemplu pentru a sublinia complexitatea operaţiilor de pace. Scopul lor este să producă condiţiile care să conducă la pace şi nu să distrugă duşmanul. Duşmanul reprezintă chiar conflictul în sine.

Transparenţa este necesară că o măsură de încredere şi de securitate. Prima companie de operaţii informaţionale pentru Statele Unite, în Bosnia Herţegovina, companie care a urmărit îndeaproape noua doctrină de operaţii informaţionale a armatei SUA, a început în octombrie 1996 în cadrul diviziei multinaţionale din nord (Task Force Eagle). LIWA (Land Information Warf are Activity) de la Fortul Belvoir, VA, a constituit punctul central al celulei de operaţii informaţionale din divizie.

Un grup de lucru pe operaţii informaţionale a inclus reprezentanţi ai G2, G3, G5, Afacerile Publice, consilieri politici, operaţii psihologice, etc. Acest grup a planificat întregul efort pentru desfăşurarea de operaţii informaţionale, a stabilit priorităţile şi a determinat disponibilitatea resurselor operaţiilor informaţionale.

Mediul de desfăşurare al activităţii aduce în prim plan noi probleme în ce priveşte informaţia şi intelligence-ul. Există multe părţi implicate şi toate sunt importante.

Toate părţile pot folosi radioul, televiziunea şi alte mijloace de informare în masă, prin care să răspândească informaţia, care poate fi adevărată, parţial falsă sau falsă.

Apoi există mediul internaţional care se concentrează pe situaţie. Toate sursele trebuie monitorizate pentru a fi avertizaţi din timp asupra situaţiei. Apoi există fluxul normal de informaţie şi intelligence. Toate acestea trebuie culese, analizate şi folosite, fie în rapoarte sau baze de date, fie pentru acţiuni directe.

Mai sunt, de asemenea, implicate şi operaţiile de securitate (OPSEC). Din nou, absenţa unui duşman clar a creat probleme de securitate. Orice salariat civil poate fi activ pentru una dintre părţi. Chiar şi cooperarea internaţională a creat unele probleme din cauza diferitelor percepţii, proceduri sau efecte ale combinării de diferite sisteme automate şi de comunicaţii. Experienţele Forţei de Intervenţie Vulturul (Task Force Eagle) aduc importante precizări conceptuale asupra organizării, folosirii şi limitelor operaţiilor informaţionale[30].

Războiul din Cecenia (1994-1996) poate furniza indici importanţi asupra complexităţii „conflictului bazat pe informaţie". Atât Rusia cât şi cecenii au folosit operaţiile psihologice (PsyOps), inducerea în eroare, managementul percepţiei şi războiul electronic. Exemplele indică că poate să existe o dimensiune specifică care merită un studiu aparte: asimetria.

Lumea super-tehnologizării se confruntă cu o dilemă. Nu se poate vorbi de progres în absenţa digitizării; dar fiecare pas spre digitizare creează noi vulnerabilităţi. Războiul este cu siguranţă mai mult decât o ciocnire de tehnologii. Este un fapt demonstrat că superioritatea tehnologică nu este o garanţie pentru victorie.

Strategii americani spun: „supremaţia tehnologică n-a putut împiedica înfrângerea Olandei în Indonezia, a Franţei în Indo- Ghina şi Algeria, a Americii în Vietnam, a Uniunii Sovieţice în Afganistan, a Rusiei în Cecenia. Toate aceste episoade confirmă faptul că superioritatea

30 Task Force Eagle.

tehnologică nu este o garanţie automată a victoriei pe câmpul de luptă, şi cu atât mai puţin la masa negocierilor”[31].

Nu este nevoie de milioane de dolari şi de sute de soldaţi pentru a ataca „Sistemul sistemelor”. Este de asemenea clar că este într-adevăr greu să dezvolţi arme noi care să-l surprindă pe duşman. Tehnologia este importantă, dar nu decisivă. Adevăratul război sau conflict este mai înainte de orice o ciocnire a voinţelor, iar în acest sens aspectele culturale pot domina.

Un lucru este cert: naţiunile şi coaliţiile trebuie să studieze adevăratele implicaţii ale operaţiilor informaţionale. Teoretic, ele pot aduce forme de conflict în care rolul războiului convenţional să fie marginal, dacă nu chiar zero. Există două cauze pentru acest luciu: caracteristicile operaţiilor informaţionale şi posibilele efecte.

Prima observaţie este costul scăzut al unui atac asupra sistemelor informaţionale şi comunicaţiilor în reţea. Acesta este de-a dreptul trivial în comparaţie cu mijloacele militare convenţionale. O combinaţie de computere şi câteva minţi strălucite şi pline de imaginaţie este suficientă.

De fapt, noi suntem azi, proprii noştri duşmani, atunci când întărim interoperabilitatea, când reducem măsurile de protecţie pentru a mări viteza, când apelăm la standardizare şi căutăm să facem economie. Toate aceste mecanisme, într-un anume fel, favorizează un intrus.

Factorul timp se reduce mai mult sau mai puţin la zero. Dacă un atac convenţional cerea timp pentru a fi organizat, iar forţele să fie pregătite şi dispuse, un atac prin computer poate să înceapă în câteva secunde după decizia lui. Acelaşi lucru se întâmplă şi cu distanţa.

La toate acestea se mai adaugă şi faptul că operaţiile informaţionale sunt realizate mai mult sau mai puţin fără vărsare de sânge. Colapsul sistemului financiar, blocarea aprovizionării cu energie sau căderea computerelor în

31 Van Riper, Paul K. şi Robert H. Scales Junior, p. 4-5.

sistemul militar de aprovizionări poate avea efecte devastatoare, dar toate acestea nu arătă – cel puţin la prima vedere – răni şi moarte.

O combinaţie a unui astfel de atac cu manipularea informaţională poate avea efecte serioase. Manipularea informaţională se poate concentra pe crearea de percepţii diferite dintre guvern şi populaţie; poate genera neîncredere la nivel guvernamental şi poate pune în pericol existenţa coaliţiilor. În cele din urmă, un guvern poate fi paralizat.

O ultimă chestiune este faptul că operaţiile informaţionale pun sub semnul întrebării conceptul separării dintre instituţiile militare şi civile şi ideile noastre de distribuţie a puterii.

CONCLUZII. Operaţiile informaţionale pot fi înţelese doar în cadrul întregului complex de schimbări. Ele nu influenţează doar sectorul militar, dar şi întreaga societate şi comunitatea internaţională. Unul dintre efectele tehnologiei informaţionale şi comunicaţionale este crearea a ceva ce poate fi numit ciberspaţiu, care este de fapt una dintre dimensiunile. În care poate fi dus războiul. Ciberspaţiul are elemente de bază inseparabile: forţele armate, naţiunea şi comunitatea internaţională. Toate nivelele de comandă şi control pot fi atacate şi în consecinţă trebuie să fie apărate. La toate nivelele, omul este cel care are puterea de decizie finală. Acest aspect face din conceptul de „influenţă” o opţiune şi un pericol. Statele moderne se confruntă cu o dilemă. Pe de-o parte, nu au nicio scăpare în faţa digitizării. Pe de altă parte, aceste progrese creează noi şi serioase vulnerabilităţi. Conceptele actuale de C2W nu sunt la curent cu dezvoltările recente. Dacă crearea „sistemului sistemelor” este răspunsul, rămâne de văzut. Ciber-terorismul şi operaţiile informaţionale sunt o adevărata problemă. Nu există soluţii uşoare. Un prim pas ar fi înţelegerea faptului că riscuri există. Un alt pas constă într-o evaluare atentă à vulnerabilităţilor. Tehnologia aduce multe foloase dar şi o taulţime de greutăţi. Există, de asemenea, şi numeroase

circumstanţe când tehnologia nu este un substitut pentru vărsarea de sânge. Operaţiile informaţionale pun sub semnul întrebării o ierie întreagă de „vechi adevăruri”. Ne confruntăm cu conflicte ţhtr-o nouă dimensiune. Avem chiar de-a face cu un nou gen de conflict.

j

ATACUL INFRASTRUCTURII CRITICE

Dr. ADAM COBB

Acest articol consideră Austtalia ca studiu de caz şi caută să răspundă la întrebări ca: unde, cum şi de ce infrastructura critică a Australiei ar putea fi supusă riscurilor. Prin examinarea elementelor vitale ale infrastructurii informaţionale naţionale (Nil – *Naţional Information Infrastructure*), cum ar fi sistemele de distribuţie a energiei, reţelele de telecomunicaţii şi financiare, este posibil a se măsura gradul de vulnerabilitate al infrastructurii.

Vulnerabilităţile evidente sunt apoi suprapuse peste o selecţie de ameninţări, prin aceasta efectuându-se o evaluare a riscurilor. Materialul va prezenta la final sugestii pentru viitoare opţiuni politice pentru guvernul australian. Articolul nu pretinde că realizează o trecere în revistă exhaustivă a vulnerabilităţilor şi ameninţărilor. Alegerea acestora s-a făcut pe baza literaturii din sursele deschise disponibile.

Tehnologia informaţiei aduce beneficii dar şi riscuri. De exemplu, folosirea computerelor legate în reţea în scopuri criminale este un fenomen în creştere care a costat deja Australia milioane de dolari. Un raport din 1997 din mediul guvernamental evidenţiază creşterea atât a numărului, dar şi a sofisticării atacurilor asupra companiilor australiene în ultimele 18 luni. Cele mai frecvente atacuri au fost asupra sistemelor financiare şi datelor confidenţiale ale companiilor.

În mod regretabil, riscurile nu se referă doar la crimele electronice. Ele includ tot spectrul, inclusiv accidente şi atacuri intenţionate. Accidentele includ dezastre naturale, probleme neanticipate (cum a fost

problema anului 2000), defecţiuni tehnice şi erori ale utilizatorilor.

Ameninţările provin din dezinformări, ură/răzbunare (din motive personale sau legate de muncă), crimă, spionaj comercial sau militar, terorism (statal sau nestatal) şi războiul informaţional, în 1998, zone din Australia şi Noua Zeelandă au fost afectate de

O severă pană de curent, când punctele cheie ale reţelelor de alimentare cu energie electrică au căzut. Aşa cum aceste întâmplări dovedesc, oraşele de astăzi sucombă rapid când reţelele lor de energie, telecomunicaţii şi financiare nu mai funcţionează corespunzător. În acelaşi ton, consecinţele unei defecţiuni ale computerelor la 1 ianuarie 2000 ar fi fost dezastruoase.

Totul, de la aparatele video din case şi aparatura cu microunde până la sistemul global de poziţionare GPS şi centralele nucleare din fosta Uniune Sovietică este supus riscului. Fiind o economie avansată, cu o forţă de muncă bine educată, cu o infrastructură extensivă, un sector de servicii puternic şi în creştere şi cu un nivel ridicat al comerţului exterior şi al finanţelor, Australia este un exemplu bun al oportunităţilor şi problemelor cu care o naţiune din O.E.C.D. se confruntă în era informaţională.

Potenţiala deteriorare a sistemelor din infrastructura informaţională critică priveşte sectorul privat şi cel guvernamental deoarece poate afecta toate elementele vieţii sociale care depind de sistemele informaţionale. Iată de ce va trebui, în protecţia Nil, sa se prevadă atât riscurile de natură accidentală cât şi cele privind deteriorările intenţionate ale sistemelor.

O mare parte din literatura despre vulnerabilităţile infra- Mructurii informaţionale s-a scris în urma apariţiei unui nou subiect în studiile strategice – războiul informaţional (R.I.). Acesta reprezintă un domeniu nou şi contestat care se referă la abilitatea Unei forţe militare de a-şi proteja sistemele de informaţii şi cunoştinţe proprii în acelaşi timp cu atacarea celor ale adversarului.

1 Yită vreme preocuparea privind infrastructura nu

este ceva nou pciltru strategii militari, noile tehnologii au schimbat felul în care Infrastructura funcţionează, ducând astfel la necesitatea reexaminării ei într-un context strategic.

R.I. a fost de asemenea asociat cu aşa-numita „revoluţie în afacerile militare” (RMA – révolution în military affairs). RMA este un concept puternic contestat, iar suporterii lui argumentează că noile aplicaţii militare ale tehnologiei de vârf asigură forţelor armate modeme progrese revoluţionare în domeniile tactic şi strategic. În acest nou context, tehnologia stealth, precizia chirurgicală, platformele cu rază mare de acţiune sunt integrate în reţele de senzori, computere şi sisteme de comandă şi control care permit o viziune foarte largă asupra câmpului de conflict.

Nemaifiind doar un spaţiu tridimensional (pământ, aer şi apă), câmpul de conflict integrează aceste dimensiuni cu altele două – spaţiul şi cyberspaţiul – unde ducerea războiului depinde de comprimarea timpului şi spaţiului. RMA se referă şi la dezvoltarea structurilor organizaţionale care sprijină optimizarea noilor tehnologii, iar de aceea a mai fost numită şi „revoluţia în afaceri de management”.

Această dezvoltare apare la un moment când în lume se petrec evenimente cu o evoluţie convergentă.

Prima, violenţa organizată se concentrează din ce în ce mai mult asupra ţintelor civile. În ultimul secol războiul a devenit nu numai apanajul guvernelor şi forţelor lor armate, ci şi al întregii populaţii civile. Pe lângă aceasta, spectrul acţiunilor teroriste se concentrează din ce în ce mai mult asupra ţintelor „soft”.

A doua, puterile statale revoluţionare folosesc adesea noile tehnologii în maniere inovative care le oferă, cel puţin la început, un avantaj decisiv în război. Acest secol a însemnat schimbări incredibile ale tehnologiei folosite în scopuri de război, de la artileria trasă de cai la rachete nucleare intercontinentale. Ca o regulă, puterile inovative au avut mai multă imaginaţie decât cele conservatoare în

dezvoltarea doctrinelor şi structurilor organizaţionale în concordanţă cu noile tehnologii. Înainte de izbucnirea celui de al doilea război mondial, generalul Douglas Haig, arhitectul războiului tranşeelor în primul război mondial, declara pompos că viitorul război va fi câştigat încă de la început printr-o şarjă decisivă de cavalerie. În 1939 exista o egalitate între aliaţi şi germani în ceea ce priveşte tancurile, aparatura radio şi avioanele.

Ceea ce a permis însă germanilor să obţină strălucita serie de victorii din 1939-1940 a fost modul de combinare a acestor tehnologii cu noile concepte tactice. „Blitzkrieg" a combinat tancurile cu aparatura radio, avioanele şi infanteria în formaţiuni militare (diviziile Panzer) prin utilizarea unor doctrine noi la care Hai g şi contemporanii săi nu se gândiseră.

A treia, sfârşitul războiului rece, care la fel ca şi sfârşitul primului război mondial, a dus la crearea unei perioade de incertitudine la nivel strategic. Deziluziile legate de politicile tradiţionale, adâncirea prăpăstiilor dintre diversele entităţi etnice şi rasiale, creşterea mişcărilor împotriva emigraţiei, insecuritatea locurilor de muncă, speculaţiile financiare pe scară largă şi incapacitatea politicilor convenţionale de a se soluţiona aceste probleme sugerează existenţa unor paralelisme între situaţia actuală din unele economii dezvoltate şi situaţia din perioada interbelică.

Aşa cum spunea E.H. Carr despre perioada 1919-1939, eşecul democraţiilor în a înţelege şi depăşi excesele distructive ale politicilor care au condus la Marea Criză au dus la apariţia unui vid la nivel politic pe care puterile totalitare l-au speculat imediat. Există asemenea paralelisme şi la nivel militar şi strategic. La fel ca în perioada interbelică, noile tehnologii există în mod curent sub forma „armelor informaţionale" dar nimeni nu a formulat încă doctrine sau structuri organizaţionale necesare pentru a traduce ta practică un „blitzkrieg informaţional".

Există astăzi o „revoluţie în afacerile militare" în aşa

multe domenii încât armele, platformele şi senzorii militari tradiţionali vor deveni mult mai puţin importante decât dependenţa informaţională în creştere a societăţii civile. Acest lucru are loc tatr-o epocă în care protecţia infrastructurii critice va fi cheia către succesul economic şi securitatea naţională. Istoria arată că, în momentele de răscruce din trecut, puterile nemulţumite au luat iniţiativa – comercială, militară sau ideologică.

În mediul actual, economic şi politic, confuz, cine va căuta noi alternative la vechile dileme va câştiga un avantaj decisiv. Conceptul revoluţionar al secolului XXI va scurtcircuita armele tradiţionale şi se va concentra pe „inima" societăţii civile – sistemele informaţionale de care depinde societatea.

Securitatea naţională implică mult mai mult decât apărarea armată. La un nivel minim, apărarea armată este fundamentală pentru supravieţuirea societăţii. Împingând definiţia mai departe, securitatea naţională se referă la crearea condiţiilor politice, economice* sociale şi de mediu înconjurător necesare unei societăţi pentru a prospera. În mod evident, un atac asupra Nil, de care societăţile dezvoltate depind mult, va reprezenta un atac la adresa securităţii acelei societăţi.

În multe cazuri, un asemenea atac va fi de departe mai devastator pentru stabilitatea şi capacitatea de funcţionare a societăţii, decât atacul asupra forţelor armate, deoarece el afectează sau distruge elementele de infrastructură cele mai importante pe care societăţile modeme se bazează mult.

Ca o consecinţă, spectrul de conflicte bazate pe informaţie reprezintă ameninţarea cea mai importantă pentru securitatea naţională de la dezvoltarea armelor nucleare acum mai bine de 50 de ani în urmă. Ca şi armele nucleare, armele bazate pe informaţie mută centrul strategic de greutate de la forţele militare la atacuri directe asupra ţintelor civile. În timp ce folosirea armelor nucleare a deevenit după 1945 ceva de neconceput, este de aşteptat ca aceste arme bazate pe informaţie să fie

folosite şi să afecteze naţiunile dependente de informaţie.

Conflictul bazat pe informaţie prevesteşte un nou tip de conflict, în care asaltul fizic la vedere, este înlocuit de infiltrări anonime şi omniprezente în societate» Nu se mai poate vorbi despre limite bine precizate, iar aceste infiltrări pot proveni din afară sau din interior. Un asalt informaţional asupra diverselor rădăcini ale societăţii nu poate fi stăvilit de o birocraţie compartimentată care este obişnuită să vehiculeze noţiuni ca divizie de cavalerie sau vase de război.

O abordare holistică, integrată, este acum necesară. Puţini au realizat în trecut că securitatea a devenit acum ceva indivizibil şi în viitor va evolua chiar mai mult, în special în contextul realizării securităţii sistemelor şi infrastructurii informaţionale de care depinde societatea.

Cu toate că preocuparea pentru securitatea infrastructurii pare a fi apărut din conceptul de RMA, ea nu ar trebui să fie în atenţia doar a strategilor militari. Aşa cum acest articol încearcă să arate, războiul în accepţiunea sa clasică este doar unul din riscurile la adresa Australiei.

Ce este Nil? În contextul acestui articol, NII este compusă din sisteme a căror incapacitate sau distrugere ar avea un impact catastrofal asupra apărării şi securităţii economice a naţiunii. Se includ aici: sistemele de telecomunicaţii, energie electrică, băncile fi finanţele, transporturile, de apă etc., atât guvernamentale, cât yi private. Din punct de vedere funcţional, ele se pot clasifica astfel:

funcţii centrale ale statului: guvern şi agenţii fundamentale cum ar fi de apărare, intelligence, afaceri externe şi comerţ, finanţe, asigurări sociale, servicii naţionale şi regionale de urgenţă.

funcţii centrale de utilităţi: reţele de alimentare, telecomunicaţii, rafinării de petrol, sisteme de transport şi stocare a gaüelor şi petrolului, sisteme de trafic şi transport (control al traficului aerian, sisteme GPS, instalaţii meteo) şi sisteme de llioientare cu apă.

r funcţiuni centrale comerciale: servicii bancare şi financiare, biass-media, sisteme de afaceri şi reţele de comunicaţii. 1 NII se sprijină la bază pe o reţea de telecomunicaţii şi este Irgfctă la infrastructura globală (GII -Global Information Infra- Itnicture) prin satelit şi cablu submarin. Ea depinde şi de o alimentare l'oristantă cu energie electrică şi de aceea elementele NII depind unul de celălalt în funcţionare, în următoarea secţiune, înainte de examinarea potenţialelor ameninţări împotriva acestor sisteme, este efectuată o analiză a vulnerabilităţilor sistemelor din NIL

Computerele, telecomunicaţiile, reţeaua financiară sau comunicaţiile militare – zone predispuse unor atacuri informaţionale – nu pot funcţiona fără energie electrică. Interdependenţa acestor componente din Nil complică eforturile de a le apăra. Complexitatea şi interdependenţa în creştere, în special a infrastructurilor energetice şi de comunicaţii, conduce la o posibilitate crescută ca o problemă minoră şi de rutină să creeze efecte în cascadă.

Distribuţia de energie în statul New South Wales (NSW) este responsabilitatea unei companii numită TransÖrid, a cărei reţea de transmisie are cca. 11500 km şi 73 de staţii şi include generatoare, echipamente de distribuţie şi 6 centre de comandă locale controlate de la centrul de control de la Carlington, o suburbie a Sydney-ului. Există două surse centrale de alimentare în stat. Una este sistemul pe bază de cărbune de la Hunter Valley, la nord de Sydney.

Celălalt este la Snowy Mountains şi cuprinde şase staţii principale situate în afară de Canberra la barajele din regiune. Energia produsă este trimisă spre Sydney printr-un singur punct, Yass. Sistemul Hunter asigură, de asemenea, alimentare alternativă pentru Sydney, dar dacă instalaţiile de la Snowy Mountains nu funcţionează, atunci probabil că sistemul Hunter nu ar putea face faţă.

Capitala Canberra este deservită de o substaţie principală care este conectată la doar două alte substaţii la Yass şi Cooma. În Canberra, cele mai multe din agenţiile

guvernamentale depind de două substaţii mai mici plasate în oraş. Computerele care deservesc reţeaua de alimentare pot fi accesate print-un număr de rute, incluzând şi sistemul de diagnostic folosit de tehnicieni pentru a monitoriza, detecta şi rezolva problemele apărute în reţea.

Din acest punct de vedere există vulnerabilităţi serioase. Prea puţine structuri din Departamentul de Apărare, de exemplu, au o sursă alternativă de alimentare cu energie electrică. În mod similar, comandamentele forţelor integrate se află în Sydney şi se bazează pe reţeaua de alimentare a oraşului, la fel ca şi legăturile dintre ele şi sediul general din Canberra.

Aşa cum a arătat explozia de la rafinăria de la Longford din 1998, sistemele de alimentare cu energie sunt vitale pentru economia naţională. Estimări recente au arătat că pierderile generate de incidentul de la Longford se cifrează la aproximativ 1 % din PNB. Oraşele principale din Australia sunt alimentate cu gaz din două sau trei surse prin intermediul unor conducte extrem de lungi care sunt controlate de computere. Aceste conducte se întind de-a lungul a câtorva mii de kilometri şi trec prin locuri nclocuite sau pe sub ocean.

Cu toate acestea, sistemele de calculatoare ce controlează funcţionarea acestor conducte nu sunt deloc supravegheate. Accidentul de la Longford ar fi putut la fel de bine să se producă tn urmă accesării sistemului SCADA (Supervisory Control and I)ata Acquisition) ce deservea rafinăria.

Există doi furnizori majori de servicii de telecomunicaţii în Australia, Optus şi Telstra. Telstra dispune de o reţea de cabluri coaxiale, fibre optice, cabluri şi fibre submarine, concentratori radio digitali. Există comutatoare dedicate de magistrală în fiecare Capitală, plasate într-o ierarhie statică. Rutele sunt testate într-o ordine stabilită, cu cea mai directă dintre ele aleasă la început. Apelurile între oraşe pot ocoli hub-urile principale doar dacă toate Unii le din hub sunt folosite.

Fiecare hub este legat cu alte capitale prin două iute

geografice |i fiecare centru de comutare al magistralei are acces către altă tiupitală. Există un număr important de puncte cheie care dacă Itint atacate, atunci toate comunicaţiile terestre între est şi vest lunt compromise.

Dacă se adaugă şi centrala telefonică de la Camooweal, atunci întregul centru al continentului ar fi afectat, cu excepţia legăturilor directe prin satelit şi a legăturilor radio de frecvenţă înaltă, în aceasta situaţie, sistemele rămase ar putea fi cu siguranţă copleşite de traficul zilnic obişnuit de date şi voce.

Australia este de asemenea un nod critic în reţeaua internaţională de fibre optice. Apelurile din şi către Australia prin cablu submarin şi satelit sunt procesate de două instalaţii din Sydney: centrala de la Paddington şi cea a lui Telstra de la Oxford Falls, în afara Australiei, există trei puncte potenţiale în Asia unde pot surveni probleme: Japonia, Honk Kong şi Singapore. Sud-estul şi nord-estul Asiei sunt conectate prin acest coridor submarin.

Legăturile spre exterior trec din Japonia spre SUA, din Singapore spre India şi apoi spre Europa. Singurul alt cablu optic submarin care asigură legătura spre SUA şi Europa trece prin Australia. În cadrul coridorului asiatic submarin, între nodurile cheie care sunt Japonia şi Singapore, Hong Kong-ul este un nod critic. Dacă acesta ar fi afectat, Asia ar fi izolată pe axa de nordsud. Dacă şi Singapore şi Japonia ar fi afectate, atunci Australia ar rămâne singura legătura internaţională funcţională din zonă. Acest lucru arată clar că Australia este un nod internaţional vital.

Reţeaua de comunicaţii prin satelit cuprinde două sisteme, unul care este parte a sistemului internaţional INTELSAT şi unul intern (Optus). Atât Optus, cât şi Telstra, funcţionează ca gateway-uri separate din reţeaua internaţională care are aproape 400 de staţii în 150 de ţări. În plus, Optus şi Telstra dispun de staţii terestre din INTELSAT, cea de la Telstra fiind o legătură importantă în reţeaua de control internaţională a sateliţilor.

Reţeaua de sateliţi Optus, conform unor surse

interne, are următoarele tipuri de funcţiuni:

componentă a sistemelor telefonice Optus şi Telstra;

reţea de management de date pentru bănci;

monitorizare la distanţă a conductelor de gaze şi petrol;

comunicaţii sol-aer şi sisteme de control al traficului aerian;

semnale de apărare;

comunicaţii mobile prin satelit;

internet;

servicii radio şi TV

Instalaţia principală de control a funcţionării sateliţilor Optus este situată la Belrose, o suburbie a Sydney-ului, cu un sistem de back-up la Lockridge. De la Belrose, sateliţii pot obţine poziţia lor pe orbită sau îşi pot modifica direcţia. Este de asemenea posibil să se acceseze şi manipuleze semnalele trimise şi recepţionate de către sateliţii Optus şi să se monitorizeze traficul de informaţii prin instalaţiile Optus. Nu există criptare pe canalul de control al seriilor A. Oricine care dispune de echipamentul adecvat poate cu uşurinţă afecta funcţionarea seriei A. În mod evident, deci, Belrose este un punct critic.

Banca centrală RBA (Reserve Bank of Australia), este responsabilă pentru stabilitatea de ansamblu a sistemului financiar. Ea este bancherul tuturor băncilor şi, în afara de supravegherea băncilor, RBA este responsabilă pentru conturile utilizate la reglementarea obligaţiilor interbancare rezultate din sistemul de plăţi. Cu alte cuvinte, decontarea cecurilor clienţilor şi transferurile electronice de fonduri sunt responsabilitatea RBA. RBA are în componenţă sistemul de transfer al informaţiilor RITS – Reserve Bank Information Transfer System, care este un sistem de reglementare globală în timp real pentru toate conturile deţinute 4e bancă.

O gamă largă de organizaţii lucrează împreună cu RBA pentru a asigura desfăşurarea corespunzătoare a operaţiunilor IBfectuate. Procesul de decontare implică colectarea informaţiilor Sflespre debite şi credite şi

stabilirea poziţiilor între instituţii. Ileglementarea se referă la „plata sau primirea valorii nete a obligaţiunilor stabilite în procesul de decontare” li Procesul de decontare este gestionat de către Asociaţia Australiană de Decontare a Plăţilor (APCA – Australian Payments Clearing Association) care este o societate cu răspundere limitată. APCA lucrează împreună cu Societatea de Telecomunicaţii

Financiare Interbancară (SWIFT – Society for World Wide Interbank Financial Telecomunication) cu sediul în Bruxelles

Aceasta înseamnă că în fiecare zi băncile australiene efectuează decontările către alte bănci prin intermediul unui computer din Bruxelles care apoi transmite rezultatele la RBA pentru reglarea conturilor deţinute de membrii APCA (de exemplu, băncile australiene). Computerul RBA este localizat în Sydney şi este legat online cu filialele RBA din toate capitalele.

Băncile au doar 45 de minute pentru procesul de decontare şi reglare în fiecare zi lucrătoare – de la 8.00 la 8.45. Rămân astfel 15 minute înainte de 9.00 pentru RBA ca să intervină, dacă este necesar, în cazurile în care o bancă nu-şi poate onora angajamentele rezultate din procesul de decontare. 45 de minute nu este mult pentru efectuarea unor intervenţii în caz că ceva nu merge cum trebuie. Sistemul bancar intern nu poate supravieţui mai mult de câteva zile dacă acest sistem delicat este afectat.

În multe situaţii în cazul tranzacţiilor electronice interne, membrii reţelei cad de acord asupra obligaţiilor bilaterale şi notifică apoi această RBA. Ca o consecinţă, toate băncile importante au centre de procesare a datelor conectate unul la celălalt şi la sistemul principal al RBA. Din motive de „eficienţă”, centrele de procesare a datelor sunt doar câteva.

Un asemenea centralism a cauzat deja probleme. De exemplu, în 1990 funcţionarea centrului de date al băncii ANZ din Melbourne a fost întreruptă când linia de alimentare cu energie a unui tramvai a intrat în contact cu acoperişul băncii ca urmare a unui accident.

Multe alte tranzacţii importante se fac prin intermediul computerului RBA. Acestea includ plăţile pe care guvernul le face către 600 de instituţii financiare, care la rândul lor distribuie aceste plăţi în conturile a milioane de australieni – funcţionari publici, membrii forţelor armate, beneficiarii de servicii sociale etc. În 1993. acest sistem a efectuat 3 milioane de tranzaţii pe zi. Aceasta reprezintă un punct slab cheie al sistepiului. Dacă, spre exemplu, în cazul apariţiei unui conflict major, un adversar ar afecta sistemul de plăţi guvernamental către forţele armate şi familiile lor, atunci moralul acestora şi al societăţii în general ar putea fi serios afectat. Acest mod de distrugere a fost evidenţiat în trecut cu grave consecinţe politice.

Criza bugetului federal din 1975 s-a transformat rapid într-o criză constituţională când guvernul a avut de înfruntat un Senat ostil, ceea ce ar fi condus la imposibilitatea efectuării plăţilor pentru armată şi nu numai. Cu toate plăţile guvernamentale făcute printr-un singur computer, securitatea financiară a milioane de australieni, precum şi stabilitatea naţională economică şi politică sunt puse serios în primejdie.

Evaluarea riscurilor este un proces care suprapune vulnerabilităţile existente peste ameninţările posibile pentru a determina ceea ce este mai probabil a se produce. Ca în multe ţări din OECD, infrastructura informaţională naţională a Australiei este supusă unor pericole intenţionate sau nu. Accidentele includ dezastre naturale, probleme neanticipate (cum ar fi problema anului 2000), defecţiuni tehnice sau greşeli ale utilizatorilor. Ameninţările includ dezinformări, ură / răzbunare (personală sau legata de muncă), crimă, spionaj economic sau militar, terorism de nivel statal sau nestatal şi războiul informaţional.

Ameninţările, cum ar fi terorismul, nu sunt neapărat mai periculoase decât cele accidentale, dacă probabilitatea de desfăşurare a unui act terorist este foarte scăzută. În anumite cazuri, probabilitatea de desfăşurare a unui

eveniment este redusă dar consecinţele surit atât de grave încât acestei ameninţări îi este acordată o prioritate mare.

Două lucruri trebuie precizate în acest context. Consecinţele linei defecţiuni apărute în NII sunt, fără îndoială, foarte grave. De fcceea vor trebui luate măsuri indiferent de evaluările probabilităţii Ameninţărilor. O dată ce probabilitatea este luată în considerare, pste clar care riscuri necesită cele mai urgente acţiuni. Al doilea, hi anumite cazuri, există o combinaţie de niveluri înalte de vulnerabilitate, o probabilitate mare de producere a unui eveniment şi consecinţe asociate severe. Oriunde există o suprapunere a acestor trei factori, există o ierarhie a ameninţărilor.

Evaluarea riscurilor efectuată în acest articol sugerează o ierarhie a ameninţărilor cu care se confruntă infrastructura critică a Australiei. Într-o ordine descrescătoare a probabilităţii şi consecinţelor asupra securităţii naţionale, avuţiei şi poziţiei internaţionale a Australiei, ele sunt:

problema anului 2000;
terorismul informaţional;
activităţi criminale majore;
dezastre naturale;
terorism statal sau nestatal;
războiul informaţional asupra sistemelor civile;
războiul informaţional asupra sistemelor militare.

Cel mai mare risc în anul 2000, asupra Nil, părea a proveni de la o „ameninţare” neintenţionată, dar cu toate acestea foarte severă. Incompatibilitatea computerelor la trecerea în anul 2000, care putea afecta computerele de pretutindeni, precum şi cipurile integrate. Căderile de sisteme datorate Y2K au impact nu doar asupra computerelor şi reţelelor individuale, ci efectele lor pot fi la fel de devastatoare ca şi un atac criminal concentrat. În mod similar, un colaps în cascadă propagat de la sistemele cu probleme, la întreaga reţea, pot ameninţa sisteme care au fost „imunizate” la Y2K.

Y2K nu accentuează doar vulnerabilităţile depistate

în Nil, dar creşte şi probabilitatea lor de apariţie. Consecinţele unor defecţiuni multiple a unor sisteme interdependente pot paraliza naţiunea mai grav decât ar putea face un atac militar.

În esenţă, problema constă în faptul că multe echipamente hardware şi programe software au fost realizate de o astfel de manieră încât folosesc data calendaristică pe două cifre. Data pe două cifre se foloseşte în milioane de fişiere de date, în milioane de aplicaţii şi în o mare varietate de sisteme hardware şi sisteme de operare.

Problema afectează cel mai mult computerele şi software-ul din echipamentele electronice. Măsurile de corecţie includ inspecţia, evaluarea, modificarea şi testarea a milioane de linii de cod, ceea ce este consumator de timp şi resurse materiale. O mare parte din gravitatea acestei probleme constă în timpul scurt ce a rămas la dispoziţie şi la gravitatea posibilelor efecte.

La 1 ianuarie 2000 orice computer care nu a fost pregătit va prezenta dificultăţi în funcţionare. Acest lucru poate avea efecte deosebit de grave dacă se are în vedere că este suficientă o singură „verigă” care nu prezintă conformitate cu anul 2000 pentru a se afecta reţele întregi. Există deci un risc deosebit de ridicat ca infrastructuri care se bazează pe computere legate în reţea să se confrunte cu defecţiuni serioase, dacă nu chiar catastrofice. Din cauză că toate se întâmplă simultan în întreaga ţară, este imposibil să se prevadă impactul global şi de aceea acesta este fără precedent.

Nu doar infrastructurile civile cheie depind de computere şi reţele. La o conferinţă recentă desfăşurată la Canberra, autorul articolului de faţă l-a întrebat pe comandantul forţelor aeriene americane, gen. Michael Ryan, dacă forţele nucleare strategice ale SUA sunt complet protejate împotriva Y2K.

Răspunsul lui a dat asigurări că toate sistemele sunt conforme cu cerinţele de trecere la anul 2000, însă mass-media internaţională pune la îndoială capacitatea Rusiei şi

fostelor republici sovietice de a se adresa ameninţărilor Y2K. De exemplu, *Sunday Times* a »portât recent că surse occidentale de intelligence au avertizat liderii politici că ar putea exista un „Cernobâl gigant” dacă problemele legate de Y2K, la nivelul sistemelor nucleare militare fi civile din fosta Uniune Sovietică, nu sunt rezolvate. Acelaşi Şiar îl citează pe consilierul preşedintelui Bill Clinton pe probleme de Y2K, John Koskinen, care a sugerat ca sistemele SUA ar putea I nu fie aşa de sigure precum declară generalul Ryan. Preocupare fi îngrijorare există nu numai la nivel militar. Bursa de valori australiană a cheltuit 12 milioane de dolari pentru a-şi verifica şi imuniza sistemele împotriva „bug-ului mileniului” şi coordonează companiile australiene în domeniu.

După ce s-a analizat ameninţarea neintenţionată care se prezintă sub forma problemei Y2K, se poate trece în continuare la considerarea ameninţărilor intenţionate. Niciuna din vulnerabilităţile discutate anterior nu ar fi importante dacă nu ar exista o ameninţare semnificativă la adresa Australiei. Trebuie de asemenea reamintit că trebuie să existe patru elemente centrale de urmărit în identificarea ameninţărilor probabile: motiv, oportunitate, capabilitate şi hotărâre.

Nil poate fi atacată în multe moduri. Există în prezent în literatura despre războiul informaţional multe discuţii foarte aprinse despre un „Pearl Harbour electronic”. Atacurile asupra Nil nu sunt aşa uşor de organizat precum sugerează unele comentarii, dar în orice caz sunt mai uşor de organizat decât s-ar putea imagina, acest lucru depinzând de ţintă şi de amploarea atacului.

Atacuri de masă asupra Nil nu sunt posibile fără o planificare şi intelligence la nivel de detaliu şi fără personal foarte calificat. Numărul mare de sisteme şi gradul de interconectare între acestea reprezintă chiar o formă de securitate deoarece nu este posibil de a face nefuncţionale aceste sisteme fără cunoştinţe detaliate despre slăbiciunile şi poziţia nodurilor critice din interiorul acestora. Doar o lovitură bine sincronizată şi coordonată

ar putea avea după aceea un efect total.

Aşa cum a fost prezentat anterior, consecinţele unui atac ar putea creşte dacă caracteristicile de redundanţă ale sistemului au fost degradate datorită imperativelor comerciale de reducere a costurilor, centralizare a nodurilor critice, reducere a operaţiunilor de întreţinere şi folosire a soluţiilor hardware/software comerciale şi comune.

Cu toate acestea, un atac în masă este puţin probabil. Chiar dacă elemente de planificare şi intelligence sunt folosite pentru atacuri informaţionale de mare amploare, aceste atacuri trebuie să fie declanşate de entităţi statale şi doar împreună cu alte forme de violenţă organizată.

Oricum, în cazul unei acţiuni militare, atacarea elementelor centrale ale NII şi centrilor informaţionali ar duce la surprindere strategică şi ar favoriza desfăşurarea în continuare a războiului convenţional.

Aceasta nu înseamnă că Australia este invulnerabilă. Dimpotrivă, un atac asupra nodurilor critice ar putea duce la o reacţie în lanţ care ar avea efecte devastatoare pentru societate. Un atac s-ar putea concentra cel mai probabil asupra unuia sau a două sisteme cheie.

Chiar defecţiuni de mică amploare ale sistemelor cheie, fără planuri adecvate de restabilire, ar putea afecta în mod serios guvernul, sectorul comercial şi societatea în ansamblul ei. Pe lângă atacul fizic, cea mai la îndemână formă de atac este interzicerea serviciului. Aceasta nu necesită penetrarea sistemelor informaţionale (pentru care sunt necesare parole sau spargeri ale codurilor sursă), ci mai degrabă supraîncărcarea nodurilor cheie din exterior (care este o formă de sufocare a sistemelor, prin aceasta împiedicându-se funcţionarea sistemului şi afectând operaţiunile sale interne.

Tehnici de info-terorism atacuri de interzicere a serviciilor;

„aranjarea” hardware-ului şi software-ului (înseamnă realizarea unor inserţii speciale în microcipuri sau în cod la momentul fabricării / programării pentru a permite

accesul ulterior neautorizat);

intruziuni în sistem (prin „spargerea” parolelor sau Exploatarea slăbiciunilor sistemului de operare);

atacuri cu viruşi de computer (bombe logice, cai troieni, viermi);

atacuri fizice (incluzând bombe cu impulsuri electromagnetice);

bruiaj şi alte tehnici de război electronic; intercepţia informaţiilor (intercepţia radiaţiei Van Eck).

Cea mai sofisticată (şi în consecinţă cea mai dificilă) formă de atac este penetrarea sistemului. Obţinerea accesului la sistem poate fi o operaţiune dificilă şi de durată. Sistemele de mare securitate, cum ar fi cele utilizate în scopuri militare sau bancare, sunt izolate de sistemele exterioare sau protejate de măsuri de securitate cum ar fi firewall-urile. Este dificil, dacă nu chiar imposibil, să se aibă acces la aceste sisteme din exterior (doar dacă cineva din interior nu a „aranjat” sistemul sau a „spart” firewall-ul).

Prin afectarea legăturilor sistemului se pierd toate avantajele legării în reţea, cum ar fi conectivitatea multiutiiizator. Uneori, acest cost este prea mare şi, surprinzător, într-un număr destul de mare de cazuri, sistemele de importanţă critică sunt legate cu alte sisteme care pot fi penetrate din exterior.

Problemele discutate anterior devin şi mai complicate în cazul infoterorismului, a doua sursă de ameninţări pentru Australia după Y2K. Interesele teroriştilor sunt bine servite de tehnologia informaţiei. Costuri reduse, dificultăţi în identificarea atacurilor şi originii lor, precum şi potenţialul haos ce s-ar crea în mediul guvernamental şi în societate în ansamblu, oferă oportunităţi deosebite pentru terorişti.

Aceştia vor fi întotdeauna atraşi de faptul că noţiunile tradiţionale de descurajare vor deveni din ce în ce mai desuete în contextul operaţiunilor informaţionale, în care un atacator (aflat poate chiar în interiorul ţării atacate) poate lansa atacuri de pe un computer mobil, mascandu-şi

sau schimbându-şi identitatea.

Olimpiada reprezintă o oportunitate deosebită pentru un terorist în viitorul apropiat, cel puţin pentru faptul că mai multe evenimente sportive de acestă anvergură desfăşurate în trecut, inclusiv München şi Atlanta, au fost marcate de acte de terorism. Instituţiile de aplicare a legii se concentrează pe securitatea fizică şi nu par preocupate de chestiuni ca cybersecuritatea. Un atac poate fi declanşat împotriva Australiei sau, la fel de bine, împotriva unei alte ţări participante la spectacolul televizat care se va desfăşură, datorită spectrului larg de ţinte şi oportunităţi ce apar în acest context. Având în vedere „spaima" creată de problema anului 2000, este posibil ca sub această acoperire să fie iniţiate acte pe scară redusă sau pe scară largă care ar putea compromite jocurile şi afecta reputaţia Australiei.

O sursă guvernamentală australiană care a dorit să-şi păstreze anonimatul a declarat *în Australian Financial Review* că guvernul federal nu a respectat în totalitate promisiunea de a dezvolta şi implementa o strategie de securitate pentru desfăşurarea jocurilor. Sursa respectivă a avertizat că Australia nu este pregătită pentru contracararea terorismului olimpic şi că acte semnificative de violenţă pot apare.

Un exemplu interesant de terorist bine educat, motivat şi fără remuşcări şi care ar fi folosit noua tehnologie a informaţiei pentru a obţine efecte sporite îl reprezintă „Unabomber" (pe numele lui adevărat Theodore Kaczynski, care şi-a câştigat „faima" în SUA timp de 17 ani prin trimiterea bombelor în colete care au ucis un număr mare de persoane).

El a publicat un manifest în care explica ceea ce l-a determinat Mă facă aceste gesturi. A fost arestat până la urmă în 1996, în urină unui denunţ. Cu resurse suficiente încât să achiziţioneze un computer şi un modem şi cu puternice resentimente împotriva »ocietăţii, un terorist de factura „Unabomber" ar putea produce pagube considerabile.

Dacă un asemenea terorist ar rămâne nedescoperit, aşa cum a rămas Unabomber, implicaţiile sociale ale actelor sale ar fi Uiajore. Un asemenea terorist ar fi capabil de descoperirea Hudurilor critice şi de ascunderea identităţii sale pentru a avea Icccs la coduri şi parole, prin aceasta câştigând acces la sistemele Vitale pentru funcţionarea societăţii.

Într-o perioadă a insecurităţii locurilor de muncă, a fri Iu cerilor alocaţiilor bugetare în multe domenii (este de amintit îi A I Inabomber era un absolvent de matematică de la Harvard) posibilitatea de a exista terorişti este ridicată în ţări ca Australia şi SUA mai mult ca oricând, în condiţiile în care tot mai multe persoane au acces la sistemele vitale din NII şi la tehnicile de atacare a acestora. Efectele acestor tehnici sunt foarte greu de imaginat dacă teroristul tip Unabomber se întâmplă să fie managerul unor sisteme critice.

A treia zonă a operaţiunilor informaţionale este reprezentată de crimă. Criminalii şi grupurile criminale organizate au sesizat rapid oportunitatea oferită de noile tehnologii ale comunicaţiei şi de nivelul de răspândire a acestora în societate. Un expert în crima organizată a declarat în *The Australian* că, cartelele crimei sunt deja cu cel puţin doi ani în faţă în ceea ce priveşte tehnologia sofisticată.

Din cele patru domenii de potenţiale ameninţări identificate anterior, crima este cea mai des întâlnită ca aplicare a tehnicilor şi strategiilor de operaţiuni informaţionale. În cadrul operaţiunilor informaţionale, tehnicile pentru atacarea unui sistem de control al traficului aerian sunt acelaşi cu cele utilizate la atacarea unei bănci. Ca o consecinţă, statisticile privind cybercrima sunt foarte folositoare, deoarece nu există dovezi clare privitoare la războiul informaţional sau acţiunile teroriste.

Biroul de evaluare a crimelor strategice (*OSCA* - Office for Strategic Crime Assessment) din cadrul Departamentului procurorului general al Australiei a desfăşurat un studiu care a cuprins 500 de companii,

departamente guvernamentale şi alte organizaţii mari şi care a urmărit să investigheze tipul, modul de desfăşurare şi frecvenţa atacurilor informaţionale pe care aceste structuri le-au suferit. Rezultatele care s-aü obţinut sugerează ceea ce se poate aştepta în viitor de la grupările teroriste şi competitorii militari.

Studiul arată ca agenţiile australiene de aplicare a legii au raportat creşteri spectaculoase atât a numărului, cât şi a gradului de sofisticare, a atacurilor exterioare asupra companiilor australiene în ultimele 18 luni. Sistemele financiare şi datele confidenţiale ale companiilor au fost două din cele mai favorite ţinte ale atacurilor. Motivaţiile atacurilor au fost: extorcarea şi terorismul (11%), spionajul (26%), câştiguri financiare (10%), producerea de deteriorări (4%) şi curiozitate (49%). Cea mai mare parte din atacuri a provenit din interior (angajaţi etc.) dar creşterea atacurilor provenite din exterior este însemnată.

Rezultatele studiului australian sunt similare cu cele obţinute în urma studiilor internaţionale. Atacatorii din exterior au folosit Internetul (25%), remote dial-în (16%) şi alte „rute” (19%). Un oficial al unei bănci importante a estimat că pierderile suferite în urma atacurilor informaţionale depăşesc 500000$.

În această perioadă Australia nu se confruntă cu ameninţări provenite de la alte state din regiune. Acest fapt reprezintă premisa de la care s-au alcătuit planurile strategice de apărare şi nu există motive imediate pentru schimbări. Tendinţele pe termen lung din regiune ridică însă semne de întrebare. O serie de ţări s-au confruntat deja cu dificultăţi financiare şi economice de neconceput cu câţiva ani în urmă.

Operaţiile informaţionale oferă mari avantaje ţărilor în dezvoltare. Mai puţin dependente de sisteme informaţionale în desfăşurarea activităţilor de zi cu zi, vulnerabilitatea lor la atacuri este mai scăzută. Având în vedere disponibilitatea pe scară largă a informaţiilor despre tehnicile folosite în operaţiile informaţionale ţi

costurile relativ scăzute de achiziţie a acestor tehnici, nu încape îndoială că operaţiile informaţionale reprezintă o opţiune atractivă.

Deoarece oferă şi posibilitatea acţionării sub anonimat, operaţiile informaţionale sunt compatibile pe deplin cu operaţiunile lUb acoperire. În contextul creşterii tensiunilor regionale, chiar Cel mai puţin dezvoltate naţiuni pot dezvolta motive, oportunităţi, tapabilităţi de a lansa atacuri informaţionale.

Operaţiile informaţionale par a oferi statelor în curs de »dezvoltare posibilitatea de a contracara asimetriile de putere dintre iele şi ţările dezvoltate. Acum aceste lucruri par doar probabile, Idar cine ştie ce se va întâmpla după în anul 2010? r Operaţiile informaţionale nu sunt o opţiune la fel de atractivă în cazul structurilor puternic dependente una de cealaltă. Consecinţele unui atac asupra sistemului financiar al statului vecin se pot răsfrânge asupra atacatorului dacă acesta depinde de sistemul în cauză.

În literatura pe marginea operaţiilor informaţionale se sugerează că folosirea acestora se face izolat de acţiunile militare. Care ar fi scopul unui atac pe scară largă asupra NII a Australiei, dacă nu preludiul unei invazii? Utilizate ca prime lovituri într-un conflict major, operaţiile informaţionale ar fi un element de surpriză cheie care ar putea afecta sistemele centrale. Acest lucru ridică o serie de întrebări privind răspunsul adecvat şi controlul escaladării conflictului. Este un asalt asupra infrastructurii financiare un act de război, presupunând ca atacatorul a fost identificat? Care ar trebui să fie riposta?

Până recent, a fost dificil să se cuprindă toate aspectele securităţii informaţionale deoarece acest lucru a fost perceput ca ceva tehnic. Însă dependenţa societăţii de sistemele informaţionale cere ca securităţii informaţionale să-i fie acordată mai multă atenţie. Deoarece Australia are multe avantaje din statutul său de economie informaţională, răspunsul trebuie să prezinte mai multe aspecte şi trebuie să se concentreze asupra exploatării oportunităţilor ridicate de era informaţională, precum şi

asupra căutării celei mai complete protecţii.

Există patru propuneri principale care pot fi cu uşurinţă implementate şi cu costuri minime. Prima este criptarea. Acest lucru ridică destule controverse în mediul guvernamental, deoarece nu este de dorit ca tehnologia să ajungă „pe mâini nepotrivite”. Criptarea oferă un nivel de securitate pentru toţi utilizatorii ce o folosesc şi teama pe care o încearcă unii este că creşterea dificultăţii de a sparge cheile criptografice va duce la creşterea dificultăţilor de a afla ceea ce zic oamenii. Fără a oferi prea multe amănunte, este suficient de spus că criptarea oferă protecţie sistemelor informaţionale.

A doua, când cineva se gândeşte la securitatea informaţională spune imediat firewall. Cu toate acestea studiile, precum şi opiniile experţilor, arată că în multe cazuri cele mai importante măsuri de protecţie încep cu proceduri simple la birouri şi acasă, cum ar fi ascunderea parolelor. Ceea ce este cu adevărat de dorit este o schimbare la nivelul „culturii de birou”, în sensul respectării cerinţelor privind securitatea informaţiilor. Cea mai bună cale de a realiza securitatea informaţiilor la nivelul corporaţiilor este desfăşurarea unor programe educative şi de instruire.

A treia, în viitorul imediat planurile companiilor trebuie să fie dezvoltate pentru a ţine cont de eventualitatea unui atac informaţional. De exemplu, dacă centrala telefonică de care depind comunicaţiile terestre ale Departamentului de Apărare este atacată, are departamentul un plan care stabileşte priorităţile de comunicaţii cu ajutorul sistemelor de rezervă? Dacă, în plus, reţeaua de alimentare cu energie electrică este atinsă şi pune în pericol sistemele de apărare?

Există un plan care stabileşte priorităţile organizaţiei astfel lhcât funcţionarea sa să nu fie prea mult afectată dacă sistemele centrale de energie şi comunicaţii sunt atinse? Aceste întrebări pot fi puse şi în cazul băncilor şi altor elemente vitale ale NII. Mai degrabă decât a dispune de soluţii la problemele anterior arătate, pare a fi mai

oportun de desfăşurat planuri la nivel erganizaţional. Acest lucru, totuşi, nu exclude cooperarea şi coordonarea, pe plan local şi internaţional, ca o practică foarte utilă în protejarea NII.

În final, ar trebui înfiinţată o Agenţie de protecţie a infrastructurii naţionale în cadrul cabinetului primului ministru. Aceasta ar trebui să cuprindă un consiliu, un centru de avertizare şi un secretariat. Rolul consiliului ar fi să coordoneze activitatea întregii agenţii şi să facă recomandări cabinetului pentru a asigura securitatea şi buna funcţionare a infrastructurii naţionale.

Consiliul ar trebui să aibă membri din ministerele şi companiile implicate în funcţionarea infrastructurii. Centrul de avertizare, partea centrală a organizaţiei, ar trebui să fie un sistem de monitorizare pe scară largă care detectează şi urmăreşte orice ncnegularitate în funcţionarea infrastructurii. Secretariatul ar trebui hfl aibă un centru de conducere, membrii săi putând proveni din Mgenţiile implicate în protecţia infrastructurii.

Există o legătură între diversitate şi conectivitate în sistemele informaţionale. Diversitatea în sistemele informaţionale induce securitate, dar complică monitorizarea în interiorul sistemului şi de-a lungul interconexiunilor între sisteme. Deoarece atacurile informaţionale foarte probabil vor fi anonime sau vor proveni de la surse cu o identitate neclară, funcţia de monitorizare trebuie să fie una esenţială. Agenţia trebuie să testeze şi să monitorizeze sistemele existente, pe baze anonime, pentru a se descoperi orice activitate suspectă. Odată ce este descoperită o neregularitate, agenţia notifică utilizatorii şi dezvoltă planuri de contracarare.

Nevoia pentru o asemenea organizaţie este recunoscută de oficialii responsabili pentru siguranţa NII din cadrul departamentului procurorului general care declara că, la un nivel minim, Australia are nevoie de „o *bază de date despre incidentele informaţionale care au avut loc... altfel va fi foarte greu de a şti dacă securitatea este la un nivel corespunzător. Similar, dacă informaţiile*

sunt distribuite, avem nevoie de un mecanism de informare a organizaţiilor cu privire la ultimele ameninţări şi tehnici de securitate"

Supravegherea activităţii agenţiei ar trebui să fie misiunea unei comisii cuprinzând reprezentanţi din mediul de afaceri şi din agenţiile guvernamentale şi al cărei rol este de a face recomandări guvernului cu privire la strategiile de urmărit. Nu este necesar, şi nici de preferat, să se creeze un minister nou pentru aşa ceva ci, mai degrabă, ar trebui ca această responsabilitate să fie acordată unui portofoliu existent.

La o primă vedere, aceasta iniţiativă nu ar stârni prea mult entuziasm.

Totuşi, tendinţele existente dovedesc că cele mai multe organizaţii aflate la partea centrală a NII realizează că actul de coordonare va fi vital atât pentru interesele lor particulare, cât şi pentru cele de grup, şi acest lucru pentru că siguranţa unora nu a fost nicicând mai dependentă ca acum de a celorlalţi. Studiul la care s-a făcut referire anterior este convingător, deoarece se bazează pe exemple atât din domeniul guvernamental, cât şi privat, şi demonstrează că cele două zone ale societăţii sunt dispuse să lucreze împreună în acest domeniu de importanţă vitală.

CONCLUZII

Ca un exemplu de stat tipic din O.E.C.D., Australia este vulnerabilă la atacurile informaţionale. Există multe noduri cheie ta NII care ar putea fi exploatate de către agresori. Interdependenţa dintre sisteme, cum ar fi cele de telecomunicaţii, energie şi reţele financiare, precum şi dependenţa sistemelor informaţionale ce funcţionează în societate, prezintă noi provocări pentru autorităţile guvernamentale şi organismele private. Criminalii şi sindicatele crimei organizate exploatează deja din ce în ce mai mult slăbiciunile din NII.

Există motive să se creadă că ameninţările posibile la adresa NII există şi ele vor creşte în intensitate pe măsură ce teroriştii şi statele agresive caută să exploateze noile

tehnologii. Cu toate acestea, există o serie de strategii care pot fi adoptate pentru protecţie.

Unele sunt soluţii simple, altele necesită o coordonare dar cu costuri de implementare destul de reduse. Elaborarea unei strategii cuprinzătoare pentru Australia prin care se caută realizarea protecţiei necesare, pe lângă creşterea robusteţii NII, reprezintă lin bun punct de plecare pentru funcţionarea economiei şi societăţii ta ansamblu în noul mileniu.

Există câteva lecţii importante desprinse din cazul Australiei pentru economiile avansate, cum ar fi cele din Europa Occidentală |i America de Nord. Dependenţa infrastructurilor critice de Computerele legate în reţea prezintă o gamă largă de provocări pentru strategii secolului XXI.

Războiul informaţional oferă imaginea unor grupuri dispersate de terorişti care beneficiază de oportunităţi de a ataca |l de a afecta (iar în cazul extrem de a distruge) fundamentele locietăţii modeme. Trebuie luate în permanenţă măsuri şi nu

RĂZBOIUL NEOCORTICAL UN CONCEPT PENTRU VIITOR

HBNRK FRIMAN[32]

În orice discuţie privitoare la războiul informaţional percepţia este elementul central şi factorul cheie al succesului. În acest material voi încerca să stabilesc dacă informaţia sau percepţia reprezintă principalul obiect al războiului informaţional Cea mai mare parte a literaturii consacrate războiului informaţional face puţine referinţe la ideea de „război al percepţiilor”.

În acest text vom vorbi despre existenţa a ceea ce s-ar putea numi război al percepţiilor şi vom încerca să descriem acest fciiomen. Vom argumenta faptul că războiul percepţiilor nu este un fenomen nou, dar de cele mai multe ori a fost luat în discuţie ca parte a altor concepte de război.

---

32 Colegiul suedez de apărare naţională, Departamentul de studii °Peraţionale.

Făcând din războiul percepţiilor obiect de studiu şi de^yăluindu-l, într-un anumit sens, sperăm să dăm o mai mare valoare conceptului. Nu poate fi negat faptul că suntem în mod constant obiecte ale atacurilor de percepţie, dar ce face din ele un fa£boi al percepţiilor? Acest material se doreşte a constitui un prim inventar al problemelor dintr-o zonă care are nevoie a fi mai bâăie cercetată.

Războiul tradiţional este o afacere de mare risc în care vieţi omeneşti sunt sacrificate pentru atingerea anumitor scopuri. Dintr-o Perspectivă umanistă, omul politic sau cadrul militar de conducere a trebuit să decidă întotdeauna dacă scopurile pot fi atinse fără a face apel la maşinăria infernală a războiului. Clausewitz ne-a învăţat că scopurile unei lupte nu înseamnă întotdeauna distrugerea forţelor inamicului şi că acestea pot fi atinse fără ca lupta să aibă loc.

În cadrul celor mai multe forme de război, iluzia victoriei sau a înfrângerii e definitorie, niciunul din participanţi nedorind să piardă. E vorba de modul în care participanţii percep evenimentele în contextul situaţiei în care se află. Războiul percepţiilor este acel concept care permite să se creeze evenimente tare produc iluzii tuturor că sunt învingători, în felul lor. Este vorba de o luptă dusă la nivelul mentalului comandanţilor.

Argumentăm în acest material faptul că ceea ce au în comun confruntările din trecut cu cele din viitor este încercarea de a }mpune voinţa asupra părţii adverse. În ţările dezvoltate violenţa fizică nu e acceptată şi societatea previne manifestarea acesteia prin toate pârghiile de care dispune.

În acest context nu este credibil să previi, pe de o parte, violenţa în societate şi pe de altă parte, să creezi forţe pentru a face faţă diverselor conflicte. Mai este mult de făcut până să vedem o lume Iară violenţă şi pentru acest lucru trebuie să vedem războiul percepţiilor ca un complement al altor forme de luptă. Ideea centrală este că cel care ia decizii va evita violenţa utilizând, pe cât posibil,

alte mijloace pentru a-şi atinge scopurile. Unei astfel de idei i se poate argumenta că atacul asupra psihicului uman, cum ar fi spălarea creierului, nu este un lucru etic şi această percepţie a atacului poate avea loc în secret, fără ca o declaraţie de război să fie făcută. Amândouă argumentele se susţin şi nu le putem nega relevanţa. Totuşi, în acest material nu vom apăra niciO poziţie privind problemele de etică, ci ne vom concentra asupra descrierii războiului percepţiilor fără a aborda şi aceste chestiuni.

Războiul poate fi văzut ca o luptă între entităţi aflate în competiţie sau ca operaţii militare între mai mulţi adversari. Scopul este de a slăbi sau a distruge adversarul. Războiul poate fi surprins tn multe forme, ca război de intervenţie, ca război de opinie sau război naţional[33]. În literatură, acelaşi interes poate fi acordat diferitelor forme de intervenţie, de exemplu, aeriană, biologică, chimică sau război informaţional. Handel[34] afirma că definiţia războiului e o problemă de nivel al analizei.

O parte a confuziei poate fi explicată prin diferenţele existente la nivelul grupurilor de lucru şi a definiţiilor. Ceea ce e asemănător pentru toate descrierile este faptul că încercăm conştient să ne atingem scopurile utilizând forţa.

Războiul percepţiilor nu este acelaşi lucru cu războiul informaţional, deşi există multe asemănări. Cu câţiva ani în urmă am încercat să descriem diferitele perspective ale conceptului de „război informaţional” (Friman, Sjöstedt and Wik, 1996)[35].

Concluzia acestui studiu a fost că filosofiile din spatele conceptului de război informaţional nu reprezintă un lucru nou, doar că noile tehnologii dau noi posibilităţi. Un exemplu este atacul unei surse de informaţii folosind informaţia ca armă. În discuţiile de până acum s-a accentuat în special aspectul tehnologic al războiului

33 H. Jomini, The Ait of War, Greenhill Books, London, 1992,

34 M. Handel, Masters of War: Classical Strategie Thought, 2 ed., Frank Cass, London, 1996.

35 într-un studiu la Swedish Institute of International Affairs.

informaţional, care asigură soluţii pentru a realiza controlul asupra fluxurilor informaţionale care înconjoară crizele.

Concepte sau tehnici de genul războiului de comandlcontrol, a războiului bazat pe informaţii, a războiului electronic, a războiului psihologic, a războiului electronic, a războiului hackerilor, a războiului informaţiilor economice şi a războiului din spaţiul realităţii virtuale au fost inventate pentru a da diferite explicaţii conceptului de rfizboi informaţional[36]. Alte concepte sunt propaganda, războiul de inducere în eroare şi dezinformarea. Elementul central al acestor concepte este lupta pentru a controla informaţia şi utilizarea ei pentru a crea intenţionat anumite efecte.

Experienţele au arătat că e dificil să controlezi producerea und activităti de război informaţional. Analizele au arătat că aceiaşi indivizi acţionează în mod diferit în circumstanţe diferite având aceeaşi informaţie, ceea ce indică faptul că informaţia disponibilă nu explică prin ea însăşi realizarea unei operaţii informaţionale şi că problema e mult mai complexă decât aceea a unei relaţii stricte dintre informaţie şi realizare.

O explicaţie a acestei complexităţi constă în faptul că fiecare individ creează „imagini" diferite în cazul aceleiaşi situaţii, care depind de starea emoţională a acestuia la momentul respectiv.

Presupunerile privind efectele în războiul informaţional sunt construite pe legea numărului mare pe care îl deţine în statistici, similar abordărilor unor afaceri generale. Produsul aşteptat este măsurat, dar nu oferă nicio garanţie că grupul va realiza în realitate, aceleaşi activităţi. În statistică interesul constă în a prevedea urmările la nivelul unui grup numeros de oameni şi e puţin hazardat a pretinde a putea prezice actele fiecărui individ în parte.

În sociologie, actele anumitor indivizi, aşa-numiţii

36 Libicki, What Is information WarfareNational Defense University, Washington, 1995.

„lideri”, vor influenţa acţiunea altora, a celor care le împărtăşesc convingerile sau care dintr-un motiv sau altul depind de ei. Pentru a crea o activitate eficientă de război informaţional ar trebui să ne concentrăm asupra liderilor care (în)direct îi afecta pe cei care-i urmează.

Credem că cel care comandă, care ia decizii este principalul punct de concentrare a activităţilor informaţionale. „Imaginea” «ituaţiei e esenţială pentru viitoarele acţiuni ale grupului sau organizaţiei şi de aceea „lupta” informaţională este, de fapt, un rflzboi al percepţiilor, o creaţie a acestei imagini.

Publicul va fi influenţat de declaraţiile liderilor şi indirect «fectat de credinţele celui care comandă. Această perspectivă se apropie de propagandă, dar diferă din punct de vedere al obiectivelor. În cazul războiului percepţiilor obiectivul este un numit element individual, în timp ce în cazul propagandei obiectivul îl constituie opinia publică.

Mao Tse Tung (*On the protracted war*; 1938) spunea odată *Cfl „pentru a câştiga trebuie să încercăm să pecetluim urechile şi ochii adversarului, să-l orbim şi să-l surzim şi pentru a crea confuzie în mintea comandanţilor adverşi şi să-i aducem în pragul* nebunieiDeclaraţia sa omagiază ceea ce noi numim războiul percepţiilor. Până acum, au fost publicate foarte puţine articole care să abordeze explicit problema războiului percepţiilor.

Una din primele referinţe este lucrarea lui Glenn şi Peterson[37], în care războiul percepţiei este explicit discutat în contextul rolului psihologiei în războiul informaţional, ceea ce pare a fi un mod des întâlnit pentru a privi problema percepţiei. Problema percepţiei e, în mod tradiţional, văzută că parte a războiului psihologic, în termeni de percepţie a managementului.

Credem că, pentru a avea succes, problema percepţiei e centrală şi nu doar în contextul războiului

37 J. Glenn, J. Peterson, Information Warfare, Cyber Warfàre, Perception Warfare and their Prévention, World Future Society, Atlanta, 1995.

psihologic sau informaţional, şi că războiul percepţiei merită să constituie un element de sine stătător şi nu doar o componentă a altor concepte, în viitor, putem avea de-a face cu un război al percepţiei. De aceea studiul acestui tip de război este foarte relevant pentru viitoarele abordări.

Conceptele războiului percepţiilor nu sunt un lucru nou, însă tehnologia care sprijină acest gen de război este foarte căutată în zilele noastre. Putem considera că preţurile, riscurile şi utilizarea eficientă a războiului informaţional pot fi foarte atrăgătoare. Avem nevoie de a arunca o privire mai adâncă asupra războiului percepţiilor pentru a-i înţelege importanţa, ca tip de război.

Pepper (1967) vedea actele de percepţie ca legături active conştiente între datele primite senzorial şi mediul înconjurător. În formele sale cele mai simple, percepţia necesită un obiect care să fie perceput şi un observator. Când spunem „văd un scaun”, scaunul este obiectul de referinţă şi „eu” este cel care observă. Filosofic vorbind, poate exista o disputa privind existenţa unei referinţe obiective, independente de datele senzoriale pe care le percepem.

Filosofii idealişti s-au confruntat cu datele, iar filosofii realişti cu independenţa celui care observă şi referinţele actului de percepţie. În funcţie de punctul de vedere pe care-l adoptăm, vom avea obiective diferite. Pepper, ca psiholog cognitiv susţine o sinteză a perspectivelor idealiste şi realiste şi realizează acest lucru concentrându-se asupra observatorului ca participant activ în procesul de percepţie, perspectivă care se concentrează asupra naturii percepţiei.

Pentru a clarifica ceea ce înţelegem prin războiul percepţiei mă voi referi la un exemplu teoretic de atac şi apărare de percepţie. Să presupunem că partea A are o sursă care îi asigură un avantaj asupra părţii B. Dacă B e interesat să limiteze acest avantaj, poate distruge efectele sursei sau poate încerca să manipuleze percepţia lui A în privinţa importanţei sursei sale în legătură cu alte obiecte.

Un ultim efort poate fi realizat prin mai multe

mijloace, dar având o baza comună: manipularea percepţiei lui A asupra sursei sale. Această manipulare poate fi realizată doar cunoscând procesul de percepţie al celuilalt. Trebuie să fim atenţi asupra modelelor care detemină natura percepţie lui.

Oamenii par să aibă capacităţi limitate de a percepe o situaţie[38]. Simon a arătat că ceea ce diferenţiază un novice de un maestru în şah este capacitatea de a vedea şabloanele în situaţiile care evoluează după structuri cunoscute, dar dacă nu este nicio Structură, maestrul nu are niciun avantaj. În mod similar, un atac asupra percepţiei este un atac asupra capacităţilor unui conducător de a găsi structuri potrivit viziunii sale asupra situaţiei date.

Pierzându-şi structura, conducătorul nu mai poate vedea şabloanele logicii. În schimb, un atac poate crea structuri care să formeze modele, care îi determină pe conducători să acţioneze tntr-un anume fel. Problema este că oamenii sunt impredictibili şi e foarte dificil să prevezi rezultatul unui atac asupra percepţiei. Totuşi, o privire în interiorul războiului percepţiilor ne dă o imagine asupra a ceea ce e important de protejat şi a ceea ce poate fi manipulat.

Miezul problemei îl constituie aflarea modului în care comandantul îşi creează propria conştientizare a situaţiei şi ce pre-înţelegere putem presupune că are. Procesul conştientizării situaţiei de către comandant şi atitudinile sale vor fi obiectivele principale ale unui potenţial atac şi elementul principal de protejat. Sun Tzu afirma: „Cine înţelege cum să utilizeze atât forţele fizice cât şi pe cele psihice, va fi victorios” (Griffith, 1971, p.82). Sun Tzu voia să spună că trebuie să vedem diferitele niveluri ale problemei care ne pot conduce spre succes. Sun Tzu conchide că un comandant aflat într-o stare de confuzie determină victoria celuilalt. Concepţia sa asupra confuziei poate fi înţeleasă ca pierderea controlului asupra situaţiei.

38 G. Miller :uThe Magical Number Seven, Plus or Minus Two", Psichological Review, 1956.

Studii recente asupra războiului modern au arătat că abilitatea de a crea sisteme de conştientizare este factorul cheie pentru a controla şi a avea succes în război. Putem descrie războiul modem că fiind lupta adevărurilor. Într-o luptă a încrederii căutăm nu doar adevărul, ci încercăm şi să-l controlăm.

O întrebare filosofică tradiţională este: ce e adevărul? Discuţiile sfârşesc de cele mai multe ori prin a concluziona că depinde de situaţie. Modul nostru de abordare a acestei probleme este că adevărul este o construcţie socială, bazată pe înţelegeri şi încredere.

Din această perspectivă, ce este adevărat pentru mine nu e în mod necesar adevărat pentru altcineva, dar de cele mai multe ori e vorba de o înţelegere asupra a ceea ce pare să fie imaginea generală a realităţii. Adevărul este atunci legat de un sistem de norme.

Conceptele tradiţionale despre războiul informaţional presupun că există un singur adevăr şi că războiul înseamnă a avea capacitatea manipulatorie de a vedea adevărata imagine a situaţiei. Însă, doar cu un singur adevăr, războiul informaţional va trebui să creeze informaţia privind maniera generală de a percepe realitatea, cu alte cuvinte, va crea ceea ce lumea crede că osie adevărat. Influenţarea sistemului de norme este un proces tare ia mult timp, ceea ce nu corespunde înţelegerii comune a iii/boiului informaţional. Războiul informaţional implică scopuri tiare, care să fie realizate într-o perioadă de timp relativ scurtă[39].

Războiul este un fenomen haotic, caracterizat de o anumită incertitudine. Primul lucru pierdut în război este capacitatea de a crea o imagine a ceea ce pare a ti adevărat. Atât observatorul cât ţi sistemul de norme vor fi afectaţi de acest lucru. Rumoarea şi dezinformarea vor face dificilă estimarea accesibilităţii informaţiei ţi decidentul va fi nevoit să acţioneze pe baza unor informaţii incomplete. În această situaţie, tot mai avem o opinie despre ce hû credem şi ce nu, fapt care se sprijină pe

39 A. Codevilla, Infonning Statecraft, 1992.

modul în care percepem fiituaţia.

Ceea ce pare să fie adevărat sau nu se va sprijini pe structurile individuale de credinţe, care se pot modifica de-a lungul timpului, tncrederea este o construcţie socială şi poate fi extinsă şi manipulată. Războiul percepţiilor nu înseamnă modificarea adevărului, ci crearea lui. În ambele cazuri, adevărul este o victimă.

Pentru a înţelege cum poate fi influenţată imaginea unui comandant asupra unei anumite situaţii trebuie să înţelegem ce lace comandantul. Într-o descriere abstractă ar trebui să vedem comandantul ca un sistem cibernetic în care acesta acţionează prin intermediul deciziilor, care se sprijină pe imaginea pe care o are despre situaţia dată. Rezultatul acţiunilor ne dă noi elemente de feed-back. Acestea schimbă imaginea asupra situaţiei, care necesită în schimb noi acte4J.

Imaginea conandantului asupra situaţiei poate li descrisă în termeni de conştientizare situaţională, bazată pe propriile-i observaţii şi pre-înţelegeri. Preînţelegerile sunt proprii fiecărui comandant şi depind de context, ceea ce explică de ce aceleaşi informaţii pot conduce la acţiuni diferite. Această conştientizare situaţională se sprijină pe factori raţionali şi emoţionali. Elementele imaginii sunt logice, din punct de vedere raţional şi al structurilor, dar unele par să fie iraţionale, având la bază emoţii. Putem descrie părţile logice în modele şi deci face predicţii, dar în privinţa părţii emoţionale avem doar sentimente intuitive.

Vulnerabilitatea reală a comandantului o constituie chiar mintea sa şi maniera în care înţelege o situaţie dată. „înrobeşte-i mintea, inima şi sufletul şi vor putea fi distruşi”. Imaginea pe care o creează mintea comandantului nu e în mod necesar adevărată, dar ea îi ghidează acţiunile.

Comandantul va continua să aprecieze cât de mult crede că are controlul asupra situaţiei, în termeni de incertitudine şi riscuri. Controlul este construit prin explicaţii logice ale situaţiei, având informaţiile structurate

potrivit diferitelor şabloane. Căutând mai multă informaţie, va încerca să limiteze incertitudinea.

În această perspectivă, războiul percepţiilor reprezintă capacitatea de a influenţa imaginea comandantului asupra unei anumite situaţii, într-un mod bine controlat, arta de a influenţa deciziile. Este important ca această influenţare să fie un proces controlat. Altfel, există riscul luării unor decizii nefavorabile.

E important de reamintit că niciun comandant nu doreşte să fie văzut ca un învins. Într-un atac al percepţiilor reuşit, fiecare participant trebuie să creadă că el e învingătorul. De aceea, scopul unui astfel de atac este de a crea iluzia (percepţia) că fiecare este un învingător.

Nu e un joc cu suma nulă, în care succesul unei părţi înseamnă insuccesul celeilalte părţi. În realitate, unii câştigă mai mult decât alţii. Percepţia situaţiei este elementul cheie al modului în care va acţiona comandantul.

Mintea este centrul de gravitaţie al unui atac. Capacitatea unui comandant de a crea o imagine satisfăcătoare a situaţiei este determinantă pentru activităţile viitoare. Adevăratul inamic în războiul percepţiilor este mintea comandantului şi nu, în primul rând, adversarul. Adversarul va încerca în orice mod să creeze o imagine conformă scopurilor sale şi cea care creează actuala imagine a situaţiei este mintea comandantului.

Întrebarea este atunci cum să ne apărăm mintea, lucru care în multe privinţe seamănă cu problema viruşilor de computer, dar care necesită găsirea altor soluţii. În lumea calculatoarelor, cea inai bună măsură de securitate este aceea de a deconecta calculatoarele de la reţele, utilizând doar calculatoare individuale cu coduri de acces. Această metoda nu e de dorit a fi folosită în cazul indivizilor care au nevoie de interacţiune socială. Trebuie găsite noi căi pentru verificare şi autorizare care să ne ajute să descoperim atacurile de percepţie.

O minte deschisă este necesară pentru a rezolva

problemele în mod creativ, dar, o minte deschisă este, în acelaşi timp, şi vu Inerabilă la interferenţe străine. Războiul percepţiilor este o luptă dusă la un nivel individual, în care comandantul este „ţinta”. Scopul este de a introduce un sentiment de nesiguranţă în privinţa problemelor pe care comandantul le consideră importante.

Nesiguranţa este concepută în termeni de pierdere a controlului. Dacă pierdem controlul, pierdem şi perspectiva a ceea ce facem pe termen lung şi riscăm să trecem de la condiţia de lider la cea de masă, care urmează un lider. Acest lucru creează oportunităţi pentru adversar în a ne condiţiona comportamentul şi deciziile viitoare. De obicei, liderul e mai uşor de identificat ca obiect, decât masa.

Pentru a putea prelua controlul, trebuie să ştim ce consideră Important comandantul (ca „observator”) şi cum putem exploata liost lucru. De exemplu, dacă acesta apreciază că a fi punctual tNte un lucru important, îi putem induce o stare de stres întârziind Informaţia. Dar nu e suficient. Cât de veche poate fi considerată Informaţia şi cât de mult poate fi considerată ca fiind de ultimă Pi A,? Problema percepţiei este o problemă de atitudine, care stă la hu/A modului în care apreciem situaţia.

Scopul final al unui război de percepţie e de a schimba modul de gândire şi modul de manifestare a voinţei. Spre deosebire de războiul tradiţional, toate părţile implicate într-un război al percepţiilor pot avea impresia că sunt învingători.

CONCLUZII

În acest material am încercat să clarificăm conceptul de război al percepţiilor. Scopul principal a fost definirea problemelor şi direcţiilor pentru o viitoare cercetare asupra acestui subiect, mai degrabă decât discutarea în detaliu a oricărei din aceste probleme. Un astfel de demers va fi făcut într-un viitor material. Totuşi, chiar şi din această discuţie introductivă ar trebui să fie clar că există multe lucruri pe care nu le ştim şi că este nevoie de multe cercetări înainte de a realiza un concept al războiului

percepţiilor. Pentru a conceptualiza ceea ce este schiţat deja, trebuie să ne concentrăm asupra unor serii de paşi şi a unor studii în această direcţie.

OPERATELE INFORMATIONALE PERSPECTIVA NATO

General maior JOSE GARDETA

Evoluţia globală a tehnologiei a schimbat lumea. Informaţia nu numai că integrează acurn cele mai multe elemente ale vieţii moderne, incluzând comunitatea civilă şi militară, dar şi accelerează toate procesele.

Această schimbare a condus la necesitatea ca NATO să examineze îndeaproape toate sistemele implicate, având mereu în vedere posibilul impact al informaţiei. Acest lucru a condus la dezvoltarea politicii NATO pentru operaţii informaţionale conţinută în documentul Comitetului Militar MC-422, care a fost uprobat de Consiliul Nord Atlantic.

Operaţiile informaţionale sunt acţiuni întreprinse pentru a influenţa factorii de decizie în conformitate cu anumite obiective politice şi militare, prin afectarea informaţiei ca şi prin afectarea proceselor care se bazează pe informaţie. Operaţiile informaţionale integrează războiul de comandă şi control cu procesul de consultare politică, aparatul de luare a deciziei şi cu operaţiile politico-militare ale Alianţei. Îi asigură comandantului o modalitate de implementare a acestui nou tip de abordare, în procesele de planificare.

În mod similar, asigură şi o concentrare a eforturilor pe âfiărare. Schimbarea operaţională importantă constă în l'oilcentrarea pe rolul informaţiei. Acest lucru include aspectele Ivmantice sau de percepţie, ca şi pe cele tehnice (*fizice şi logice*). *Planificarea militără nu necesită numai implicare directă a njmratului politic de luare a deciziei, dar şi o implicare şi o integrare Inrgă a unor elemente din conducere.*

Subiectul „operaţii informaţionale" devine tot mai critic pe zi ce trece, pentru naţiuni. Operaţiile informaţionale au capacitatea de a atinge inima unei

naţiuni, să aducă prejudicii infrastructurii, să aducă atingere acelor lucruri care-i permit unei naţiuni să existe.

Unul dintre cele mai mari câştiguri, ce poate ô exploatat de pe urma folosirii operaţiilor informaţionale, este abilitatea lor de a preveni dezvoltarea unei crize în conflict prin mijloace şi metode care demonstrează potenţialului adversar că escaladarea respectivei crize nu este în interesul său. În acest sens, activităţile trebuie să fie conduse pe timp de pace şi ar trebui să fie sprijinite atât poliţie cât şi militar, să cunoască atât punctele tari cât şi cele slabe şi să se concentreze pe acele zone care sunt Cele mai eficiente în atingerea obiectivului final.

Probabil că cel mai îngrijorător aspect în dezvoltarea operaţiilor informaţionale este faptul că nu ekistă o înţelegere generală â ceea ce sunt acestea cu adevărat. Cd mai mtilti suht familiarizaţi cil diferite părticelepe care le cbnsâderă din păcate că reprezentând întregul: Olanda recunoaşte importanţa operaţiilor informaţionale ca şi importanţa implicaţiilor lor. Un indice important al acestei înţelegeri esté studiul bilateral întreprins de Olanda şi de Germania.

Operaţiile informaţionale nu sunt un concept nou, de sunt rezùltatul evoluţiei eforturilor noastre în dezvoltarea sistematică a abordării războiului. Manifestări mai moderhe ale evoluţid se găsesc expuse de către Von Clausewitz în caftea sa, „Despre război” unde autorul discută principiile războiului.

Màijrecent este însă conceptul Statelor Unite, Joint Vision 2010, în care este abordată o nouă modalitate de implementare a cerinţelor operaţiilor informaţionale. Aceste aspecte, precumsi alte numeroase încercări de organizare eficientă a armatelor, plus tehnologia informaţională, ne-au condus astăzi la adoptarea prezentei poziţii.

Înainte de a ne concentra analiza asupra operaţiilor informaţionale, voi aminti strategia care a condus dezvoltarea operaţiilor informaţionale, o strategie caje a fost executată aproape perfect de către aliaţi în războiul

din Golf. Această strategie este comanda şi controlul.

Războiul de comandă-control este definit în MC-348, „Politica războiului de comandă-control”, astfel: „*Folosirea integrată a tuturor capacităţilor militare, inclusiv operaţiile de securitate* (*OPSEC*), *inducere în eroare, operaţii psihologice* (*PSYOPS*), *război electronic* (*EW*) *şi distrugere fizică sprijinită de către toate sursele de intelligence şi CIS, pentru interzicerea accesului la informaţie, influenţarea, degradarea sau distrugerea capacităţii* C2 *a unui adversar în timp ce sunt protejate toate acestea împotriva unor acţiuni similare*”.

Cu alte cuvinte, războiul de comandă-control înseamnă exact ceea ce afirmă şi denumirea sa, executarea de acţiuni pentru prevenirea controlului adversarului asupra informaţiei necesare pentru realizarea de evaluări şi decizii corecte privind controlul şi folosirea bunurilor sale.

Figura 1 ilustrează cum cei cinci piloni ai războiului de comandă-control sunt discipline individuale, iar atunci când există coordonare şi sprijin ferm din partea intelligence-ului şi comunicaţiilor, întregul pe care ei îl produc, războiul de comandăcontrol, este mult mai mare decât suma tuturor părţilor.

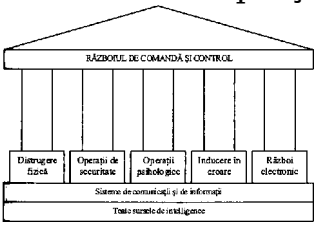


Figura 1: *Cei cinci piloni ai războiului de comandă-control*

Războiul de comandă-control se referă la coordonare. Prin folosirea celor cinci piloni şi a altor capacităţi militare într-o manieră coordonată, se obţine o sinergie care permite operarea extrem de eficientă în cadrul unei crize/conflict. Operaţiile informaţionale nu înlocuiesc războiul de comandă-control, dar integrează această

strategie militară în procesul de consultare politică, în aparatul de luare a deciziei şi le combină cu operaţiile politice şi militare ale Alianţei.

Cu alte cuvinte, războiul de comandă-control este aplicarea militară a operaţiilor informaţionale. NATO are o experienţă considerabilă cu războiul de comandă şi control şi-l execută ireproşabil. Alianţa a aprobat politica în MC-348 încă din 1995, şi de atunci fiecare OPLAN a conţinut o anexă de război de comandă şi control.

În timp ce războiul din Golf este în general recunoscut ca primul război informaţional, nu atunci s-a folosit pentru prima dată războiul de comandă-control în luptă. De-a lungul secolelor, comandanţii au ştiut că impiedicarea adversarului de obţinere a informaţiei este un excelent mijloc de sabotare a campaniei sale.

Cum se poate în acest amestec de informaţie ca pe de-o parte să prevenim ca informaţia critică să ajungă la inamic, în timp ce pe de altă parte să prevenim efectul opus? O bună parte din răspuns rezidă în planificarea la toate nivelele operaţionale şi tactice. Dar azi, în actualul mediu internaţional, planificarea nu trebuie să fie strict delegată sectorului militar, şi această afirmaţie se referă îndeosebi la NATO,atunci când se are în vedere faptul că toate capacităţile militare ale NATO derivă din cele 19 naţiuni, efectele pe care operaţiile informaţionale le pot avea asupra NATO devin clare.

Operaţiile informaţionale sunt interesate de obiective informaţionale, pe care un comandant caută să le atingă prin acţiunile sale. Operaţiile informaţionale au impacturi diferite la diverse nivele de război, din moment ce fiecare nivel este diferit. La nivel strategic, operaţiile informaţionale sunt folosite în sprijinul obiectivelor NATO. Acest sprijin este obţinut prin influenţarea sau afectarea tuturor elementelor (politice, militare, economice sau informaţionale) a puterii naţionale a adversarului, în timp ce sunt protejate cele ale NATO.

La nivel operaţional, operaţiile informaţionale se concentrează pe sprijinul obiectivelor operaţionale majore.

Impactul major la acest nivel este simţit de către liniile de comunicare, logistică şi comandă-control ale adversarului. La nivel tactic sprijină îndeplinirea obiectivelor tactice specifice.

O definiţie a operaţiilor informaţionale, aşa cum reiese din MC-422, care este intitulată „Politica NATO a operaţiilor informaţionale”, aprobată de către Comitetul militar pe 15 decembrie 1998 şi de către Consiliu pe 22 ianuarie 1999: operaţiile informaţionale sunt definite ca *„acţiuni întreprinse pentru a influenţa factorii de decizie care sprijină anumite obiective politice şi militare*; *prin afectarea informaţiei altora*, a *proceselor care se bazează pe informaţie*, *a sistemelor* C2 *şi CIS în timp ce exploatează şi protejează propria informaţie şi propriile sisteme informaţionale*.” Există două categorii principale de operaţii informaţionale: operaţiile informaţionale defensive şi operaţiile informaţionale ofensive.

Unele dintre capacităţile folosite în cadrul operaţiilor informaţionale defensive includ: asigurarea informaţiei, operaţiile de securitate (OPSEC), securitate fizică, contra-inducere în eroare, contra-propaganda, contra-intelligence şi război electronic. Operaţiile informaţionale ofensive pot de asemenea să sprijine operaţiile informaţionale defensive. Sistemele informaţionale servesc drept înlesnitori, care întăresc capacităţile de luptă; faptul că NATO se bazează tot mai mult pe aceste sisteme creează vulnerabilităţi.

Este imposibil să protejezi complet toate sistemele, tot timpul. De aceea trebuie protejate bunurile relative la valoarea informaţiei pe care le conţin şi riscurile asociate cu pierderea sau degradarea acelei informaţii. Această valoare va varia bineînţeles în timp.

Există mai multe procese implicate care interrelaţionează cu operaţiile informaţionale defensive, şi care includ protecţia mediului informaţional: capacitatea de a detecta atacuri asupra sistemelor; capacitatea de a restaura sistemele pentru a putea folosi acest tip de atac şi de a avea capacitatea de a răspunde unui astfel de atac.

Operaţiile informaţionale ofensive implică folosirea integrată a capacităţilor şi activităţilor desemnate, sprijinite de intelligence, cu scopul de a afecta factorii de decizie adverşi şi de a obţine şi promova obiective specifice. Capacităţile folosite în acest scop includ, dar nu sunt limitate numai la, operaţii de securitate (OPSEC), inducere în eroare, operaţii psihologice (PSYOPS), război electronic (EW), atac fizic/distrugere şi atac asupra reţelei de computere.

După părerea mea, NATO va acţiona, în special în situaţii de răspuns la criză şi datorită naturii alianţei care are nevoie de consensul celor 19 naţiuni suverane pentru a proba şi implementa acţiunile. Sistemele naţionale juridice complică şi mai mult această problemă, din moment ce, în unele cazuri, unele activităţi sunt considerate a fi ilegale.

Cred că înseamnă folosirea tuturor capacităţilor care sunt la îndemână pentru protecţia propriei informaţii, a sistemelor şi proceselor care se bazează pe informaţii, în timp ce se încearcă atingerea celor ale adversarului. Atunci când sunt analizate capacităţile, cel mai potrivit punct de plecare este războiul de comandă şi control: războiul electronic, operaţiile de securitate (OPSEC), inducerea în eroare, distrugerea fizică şi operaţiile psihologice (PSYOPS). A nu se confunda: operaţiile informaţionale înseamnă mai mult decât cele cinci elemente ale războiului de comandă şi control.

Lanţul de comandă se extinde mult şi la nivelul adversarului şi la conducerea sa civilă. În mod cert, ramificările folosirii majorităţii capacităţilor războiul de comandă şi control împotriva unei naţiuni constituie un act de război. Dar tot atât de clar este şi faptul că dacă, conducerea părţii adverse de la acel nivel poate fi afectată, un conflict iminent poate fi evitat. Dar, pe timp de pace, conducerea politică nu este o ţintă militară legitimă. Astfel se poate vedea dilema cu care se confruntă planificatorii militari pe măsură ce ei continuă să dezvolte procesul C2W.

Operaţiile psihologice au un loc special în cadrul

războiului de comandă şi control şi al operaţiilor informaţionale, din mai multe motive. Printre altele, furnizează militarilor mijloacele de influenţare a conducerii adversarului, a trupelor sau chiar a populaţiei, pe timp de pace.

În ciuda acestei capacităţi, pe care eu o consider ca o punte între războiul de comandă şi control şi operaţiile informaţionale, operaţiile psihologice sunt aşa de maligne încât doar simpla lor

Î

enţionare în anumite cercuri conduce la reacţii nefavorabile, cest lucru este valabil, mai ales în mediul politic. Membrii acestor Instituţii înţeleg trei puncte importante despre relaţia dintre operaţiile psihologice şi aducerea la cunoştinţă pentru publicul jarg, a diferitelor informaţii.

În primul rând, operaţiile psihologice sunt acuzate de planificarea şi executarea proiecţiei de activităţi care intenţionează.sa informeze persuasiv grupurile ţintă şi populaţia. Intenţia operaţiilor psihologice nu este propaganda sau minciuna ca furnizarea informaţiilor adevărate sau a declaraţiilor atunci când intçresele noastre sunt cel mai bine servite. De fapt şi de drept, minciuna este contra productivă pentru că o dată descoperită toată credibilitatea este pierdută.

j Atunci când sunt folosite aşa cum trebuie, tehnicile operaţiilor psihologice pot scădea moralul şi reduce eficienţa forţelor duşmane şi pot crea dizidenţă. În al doilea rând, operaţiile psihologice şi informarea publicului larg trebuie să se coordoneze. Operaţiile psihologice au un impact major asupra fluxului de informaţie. Momentul în care se produce informarea publicului poate fi modificat astfel încât să vină în sprijinul percepţiilor Miibilite de către operaţiile psihologice.

În cele din urmă, operaţiile psihologice executate pe timp de pace vor avea o altă concentrare decât atunci când sunt folosite pe timp de criză sau conflict. Eforturile pe timp de pace se concentrează pe operaţiile militare altele

decât războiul, precum Operaţiile de Sprijin al păcii (PSO), asistenţa umanitară şi sprijin în caz de catastrofă naturală. Pe timpul conflictului, operaţiile psihologice sunt folosite ca orice altă capacitate de sprijin a realizărilor obiectivelor comandantului.

Partea politică a Alianţei ar trebui să vadă operaţiile psihologice ca partener al activităţilor de informare publică, şi nu ca un competitor, şi în mod cert nu ca o maşină de propagandă. Operaţiile psihologice sunt o capacitate pur militară şi de aceea nu pot să fie înlocuite sau subordonate informării publice. Aşa cum am afirmat şi mai devreme, planificarea şi coordonarea folosirii operaţiilor psihologice şi informării publice au potenţialul de a preveni izbucnirea ostilităţilor.

Digresiunea noastră asupra operaţiilor psihologice nu a fost în zadar. A adus în mod subtil în discuţie un alt fapt care, în opinia mea, este cel mai important aspect al operaţiilor informaţionale.

Acum că am văzut de unde a provenit conceptul NATO de operaţii informaţionale şi cum l-am definit, aş dori să vă răpesc, puţin din timpul dumneavoastră, pentru a analiza cum se pot implementa operaţiile informaţionale. Cred, de asemenea, că este absolut necesar să subliniez câteva schimbări fundamentale care au avut loc în ultimii zece ani, şi care au influenţat în mod semnificativ modul în care armatele NATO fac faţă crizei sau conflictului.

Evoluţia globală a tehnologiei în domeniul informaţiei a schimbat lumea. Informaţia nu numai că a integrat cele mai multe elemente ale vieţii moderne, dar a şi accelerat toate procesele. Viteza cu care putem să transmitem informaţia, volumul de informaţie sunt fără precedent. Azi avem posibilitatea a trimite o cantitate aproape nelimitată de informaţie, în numai câteva secunde. Miniaturizarea computerului a făcut din el un echipament standard, chiar şi pe câmpul de luptă.

Tehnologia este doar unul dintre regimurile operaţiilor informaţionale. Un alt aspect pe care l-am atins puţin atunci când am discutat despre operaţiile

psihologice. Acesta este regimul semantic sau cognitiv. Partea tehnică este probabil mai bine înţeleasă probabil decât cea semantică deoarece implică lucruri cu care suntem obişnuiţi, echipament şi folosirea sa.

În timp ce operaţiile informaţionale se concentrează pe soluţii non-kinetice, trebuie să avem mereu în vedere că distrugerea fizică, unul dintre cei cinci piloni ai războiului de comandă şi control, este de asemenea un element al operaţiilor informaţionale. Partea cognitivă include capacităţile găsite în informarea publică, operaţiile psihologice şi operaţiile mass-media.

Războiul rece a furnizat Alianţei,,o situaţie de planificare ideală": perioade lungi de tensiune, zone cunoscute de angajare, adversari cunoscuţi şi înţeleşi. Principala funcţie a aparatului politic în ce priveşte conflictul era să decidă dacă NATO trebuia Sau nu să se implice, şi dacă da, să declare implicarea sa. Exista puţină implicare politică o dată ce conflictul era declarat şi se desfăşura.

Azi, circumstanţele diferă considerabil. Aşa cum s-a demonstrat şi prin operaţiile forţei aliate, NATO este azi constrâns de implicarea politică în timpul unei crize. Acest lucru înseamnă cft autorităţile politice controlează sectorul militar. Militarii trebuie sfl se mişte în mediul creat de politicieni.

Un bun exemplu al acestei situaţii rezultă şi din declaraţia Alianţei că nu va folosi trupe terestre pentru conflictul din Kosovo. În mod cert, această decizie a fost o manevră politică din partea NATO. Impactul acţiunilor militare asupra sensibilităţilor, implicaţiilor şi imperativelor politice în conducerea operaţiilor trebuie să fie pe deplin înţelese atât de structura militară cât şi de cea politică.

O altă variabilă care trebuie luată în considerare este »enzitivitatea naţională. Sensibilităţile naţionale au fost o grijă majoră a NATO, şi aşa şi trebuie să fie într-o alianţă în care deciziile se bazează pe consens. Cu toate acestea, în zilele războiului rece, aceste sensibilităţi nu aveau un

impact prea puternic asupra stipulărilor articolului V şi asupra alocărilor de resurse naţionale pentru NATO, aşa cum se întâmplă azi în era informaţională.

Aşa cum am menţionat mai înainte, multe dintre resursele noastre au fost croite pentru a veni în întâmpinarea cerinţelor tipurilor de scenarii din articolul V, pe care NATO le planifică de ani de zile.

Două exemple a celor mai importante resurse la care fac referire sunt capacităţile operaţiilor ofensive şi intelligence. Aceste capacităţi sunt foarte atent păzite de către naţiuni, ceea ce înseamnă că acestea vor ezita în a aloca resurse Alianţei.

Un alt factor important, pe lângă sensibilităţile naţionale şi legătura lor cu alocarea de resurse este opinia publică. Azi scene de luptă intră în casele noastre aproape fără întârziere; războiul aşa cum este văzut de CNN este o regulă, în mod evident, opinia publică este extrem de importantă pentru politicieni şi va afecta cu siguranţă deciziile lor în ce priveşte resursele.

O altă şi ultimă schimbare, pe care o vom lua în discuţie, şi care pentru noi militarii este mai uşor de înţeles deoarece ne confruntăm cu ea în fiecare zi, este intelligence-ul. Planificarea, executarea şi evaluarea activităţilor de operaţii informaţionale este imposibilă fără un sprijin adecvat din partea intelligence-ului. Acest lucru pune însă Alianţei o serioasă problemă, deoarece ea nu posedă capacitatea organică de a aduna şi procesa datele cerute pentru dezvoltarea intelligence-ului.

În plus, nu există un aparat politic/militar de intelligence în funcţiune în cadrul NATO. Şi pe deasupra, cerinţele de intelligence pentru operaţiile; informaţionale sunt diferite faţă de cele care se găsesc în mod tradiţional în armată.

Intelligence-ul trebuie să fie la timp, precis, uşor de folosit, complet, relevant, la obiect şi suficient de detaliat pentru a sprijini cerinţele NATO. Operaţiile informaţionale au nevoie de răspuns la o întrebare pe care comunitatea de operaţii nu a mai pus-o niciodată intelligence-ului: de

ce? În trecut erau necesare „doar faptele” în lumea operaţiilor informaţionale, acest gen de informaţie nu mai este suficientă pentru a face o treabă bună.

Intelligence-ul contribuie de asemenea şi la procesul de detectare a atacului prin furnizarea de avertismente, prin evaluarea activităţii potenţiale a adversarului şi prin culegerea de indici specifici de activitate.

În plus la toate acestea, comunitatea operaţională trebuie să fie foarte precisă în descrierea cerinţelor comunităţii de intelligence. Un prim pas în dezvoltarea cerinţelor de intelligence constă în determinarea de unde vor veni ameninţările pentru NATO. Apoi este necesară determinarea dacă acea naţiune sau acel grup anume posedă capacitatea de a întreprinde operaţii informaţionale.

Pe scurt, datele problemei pentru NATO s-au schimbat în mod dramatic, faţă de acum 10 ani. Lumea militară nu trebuie doar să accepte acest lucru, ci să se şi adapteze la aceste schimbări.

În mod cert, situaţia descrisă mai sus are un impact de proporţii asupra operaţiilor militare, incluzând şi operaţiile informaţionale. Acest lucru este adevărat mai ales la nivel strategic politic/militar. Aşa cum am menţionat şi mai înainte operaţiile informaţionale ale NATO nu trebuie considerate ca fiind o nouă strategie. Dar viteza şi volumul cu care transmitem informaţia, precum şi aria de aplicabilitate au schimbat complet impactul general al Informaţiei asupra interfeţei politice/militare.

Ce înseamnă toate aceste lucruri pentru NATO şi cum poate A lianţa să profite de oportunităţile oferite de operaţiile informaţionale? (li mod cert, primul pas este elaborarea unui plan. Pentru acest plan latţ important să păstram în minte toate condiţiile noi.

În primul rând trebuie să ne antrenăm liderii şi personalul cu Mtri cheie pentru a fi în măsură să gândească diferit.

Trebuie să înţelegem că documentaţia nu ne va furniza întotdeauna certitudinile cu care suntem obişnuiţi

sau pe care le căutăm. Prezenta situaţie şi orientarea politică vor dicta cum vor acţiona şi reacţiona militarii într-un conflict.

Una dintre cele mai importante lecţii care ne-au fost date de Kosovo, constă în faptul că armatele se mişcă într-un mediu creat de politicieni. La rândul lor, politicienii trebuie să înţeleagă consecinţele militare ale deciziilor pe care le iau.

Să ne întoarcem acum la planul pentru operaţiile informaţionale ale NATO. Structura nivelului de lucru de fiecare zi este în funcţie. Trebuie acum să dezvoltăm mecanismul de ghidare şi direcţionare a programelor pentru a obţine un beneficiu maxim pentru Alianţă. În acest scop, am stabilit:

Grupul de lucru NATO pentru Operaţii informaţionale. Acest comitet este prezidat de un'Plag Officer, şi are membrii permanenţi: naţiunile, comenzile strategice (SC Strategic Comands), un preşedinte pe probleme juridice pentru zonele funcţionale, care cuprind elemente de război de comandă-control, de exemplu operaţiile informaţionale, conducerea internaţională/ treburi politice şi Subcomitetul NATO de securitate informaţională (INFOSEC).

Pe timpul participării noastre la campania de operaţii informaţionale din Kosovo, a devenit limpede că nu există o înţelegere comună a operaţiilor informaţionale sau a cerinţelor pentru stabilirea unei campanii. Dezvoltarea avertizării timpurii este extrem de importantă în acest context.

Noi am mai realizat ceva şi în partea defensivă* cea care este administrată de către NHQC3S.

Conducerea C3 a NATO a început să studieze multe aspectc ale operaţiilor informaţionale. Ea a însărcinat Subcomitetul INFOSEC să dezvolte viziunea NATO de asigurare a informaţiei. Discuţiile în această zonă s-au concentrat pe rolurile Comitetului Militar şi ale NG3B via INFOSEC SC. Un dbcurnent care tratează problemele ridicate de asigurarea cu informaţii este acurtf în cea de^-

a doua sa revizie. Pè lângă aprobarea SC, acest document va li înaintat spre aprobare lui NC3B.

În plus, NC3B a însărcinat Subcomitetul INFOSEC cu dezvoltarea implementării planului pentru CERT (Computer Emergence Response Team). Această echipă va asigura utilizatorilor CIS avertizări prompte la adresa securităţii lor şi sfaturi. Realizarea unei astfel de echipe va avea impact atât asupra mediului militar, cât şi civil a organizării NATO.

Din nou trebuie amintit că dezvoltarea avertizării de timpuriu este extrem de importantă. Mijloacele primare prin care urmărim dezvoltarea acestei capacităţi sunt cursurile la şcoala NATO, SHAPE, participarea la forumurile naţionale, la seminariile profesionale şi la grupurile, organismele şi agenţiile NATO. Participarea noastră la Simpozionul din Academia Militară Regală a Olandei, din 3 decembrie 1999, este un exemplu.

Operaţiile informaţionale trebuie să devină o parte integrantă u procesului de planificare operaţională. Operaţiile informaţionale sunt aplicabile în orice fel de condiţii, de la pace la criză şi război şi înapoi la pace. Lor le este furnizată orientare politică clară din partea Consiliului, şi vor juca un rol cheie atunci când sunt implementate toate aspectele conceptului.

Mai trebuie să ating şi aspectul dependenţei evidente a NATO de capacităţile naţiunilor, de exemplu intelligence, capacităţi care sunt vitale pentru planificarea şi conducerea de operaţii informaţionale.

Unele dintre capacităţile operaţiilor informaţionale ofensive dezvoltate de către naţiunile membre ale Alianţei sunt foarte mnsibile şi destul de scumpe, şi de aceea nu vor ti asigurate de către naţiuni. De aceea este prudent din partea NATO să-şi dezvolte nişte capacităţi organice ofensive.

Operaţiile informaţionale pe timp de pace, dacă sunt doscoperite de către ţintă pot foarte bine să fie considerate provocatoare, ba chiar ostile, şi pot de aceea să necesite autorizare politică clară din partea Consiliului.

Două din cele mai importante componente ale operaţiilor informaţionale, intelligence-ul şi comunităţile de CIS, vor îi foarte mult implicate în determinarea şi abordarea ameninţărilor sistemelor noastre şi a vulnerabilităţilor sistemelor noastre la aceste ameninţări. Ca un minim necesar, este de dorit ca noi să determinăm sistemele critice care trebuie protejàte pentru a putea proteja funcţionarea pe mai departe a NATO.

Cu scopul de a verifica şi pune în practică aceste proceduri este necesar să includem operaţiile informaţionale în cadrul exerciţiilor NATO.

Dezvoltarea unei doctrine de operaţii informaţionale trebuie să fie iniţiată cât de curând. Doctrina este un compendiu de lecţii învăţate. Operaţiile în Balcani vor furniza cu siguranţă un material excelent pentru acest document. Să ne amintim mereu că operaţiile informaţionale sunt un mod de gândire şi nu neapărat ceva Uşor de cuantificat.

CONCLUZIE. În concluzie, permiteţi-mi să mai subliniez încă o dată că operaţiile informaţionale nu sunt ceva nou. Ceea ce este nou este procesul de gândire, pé care-l mandatează operaţiile informaţionale.

A INFORMA, CHIAR ÎN CONDIŢII DIFICILE..

Col. EDWIN HOFSTETTER Elveţia într-un stat democratic, cum este şi Elveţia, cenzura massmedia este ceva de neconceput. Guvernul elveţian a decis să creeze un,»regiment informaţional" care să acţioneze dacă, în anumite circumstanţe, activitatea normală a presei, radioului şi televiziunii este pusă în pericol. Acest articol descrie istoria, misiunile şi organizarea acestui regiment.

În anii de dinaintea celui de al doilea război mondial, circumstanţe politice dificile influenţau eforturile de informare a populaţiei şi forţelor armate. Instituţiile germane erau în plină desfăşurare a unei bătălii de propagandă la o scară mare, chiar şi împotriva Elveţiei.

Majoritatea presei elveţiene reuşea să combată această propagandă, reflectând libertatea şi autonomia ţării. Guvernul şi armata au încercat, prin îndrumare şi

control, să prevină apariţia unor provocări la adresa Germaniei. La izbucnirea războiului, acest lucru a condus la cenzurarea presei.

O dispoziţie a armatei în toamna lui 1939 a creat secţiunea „Heer und Haus" (Armata şi Casa). Această organizaţie avea misiunea de a informa populaţia despre chestiuni legate de up&rarea naţională, cu scopul de a întări rezistenţa naţională şi de îi menţine identitatea naţională. O reţea cu mai mult de 100000 de membri şi 7000 de corespondenţi din întreaga ţară activa pentru Informarea, în diferite limbi, a populaţiei elveţiene, reuşind în acest mod să ia şi pulsul societăţii.

O altă structură, „Action National Resistance44 – Rezistenţa naţională pentru acţiune, de această dată privată şi neafâliată politic, completa acţiunile „Heer und Haus". Acţiunile acestor structuri erau coordonate de serviciul de intelligence şi biroul de presă şi radio al guvernului. La puţin timp după terminarea celui de al doilea război mondial o nouă organizaţie privată a hiat fiinţă: S wiss Information Service (Schweizerische Auflarungsdienst – SAD).

Îii anii de dinaintea celui de al doilea război mondial, statul major elveţian a luat o serie de măsuri de prevedere, cum ar fi controlul presei. Când războiul a început, în 1939, armata a stabilit că ar trebui să existe o cenzură preliminară. Guvernul elveţian, Bundesrat, a anulat această măsură şi a decis că cenzura va funcţiona doar după publicare.

Discuţiile cu reprezentanţii ma&s-media au dus la apariţia unor reglementări, în concordanţă cu legile constituţionale şi starea de război. La început, armata era responsabilă pentru cenzură şi aplicarea acestor reglementări. Prin aceasta, departamentul presă şi radio (Abteilung fur Presse und Rundfunk -APF) din statul major avea scopul de a proteja securitatea internă şi externă a ţării şi neutralitatea sa, era responsabil de monitorizarea publicaţiilor şi transmiterea mesajelor şi opiniilor prin telegraf, telefon, presă, radio, filme şi imagini. Şeful

statului major, gen. Guisan, nu considera însă cenzura presei ca o misiune a armatei ci, mai degrabă, ca o treabă politică.

Ca o consecinţă, în 1942 APF a fost subordonat directorului departamentului elveţian pentru justitie şi poliţie. Organizarea militară a APF a fost menţinută şi nu a fost modificat modul de realizare al cenzurei. Rapoartele şi comentariile de politică externă au fost în special urmărite.

Editorii erau avertizaţi şi unele ediţii ale ziarelor erau oprite. Bundesrat-ul putea interzice publicarea unui ziar dacă considera că urmările acestei publicări ar impune. Aceste măsuri extreme au fost aplicate de aproape 60 de ori în cel de-al doilea război mondia I

Într-un stat democratic, cum este Elveţia, cenzurarea mass mediei este astăzi ceva de neconceput. Lecţiile învăţate în timpu I războiului şi noile tipuri de ameninţări ale războiului rece au materializat ceea ce se numeşte „apărarea totală” Acest concept include, de asemenea, şi comunicaţiile, acestea trebuind să rămână sigure în caz de război, acţiuni teroriste sau catastrofe. APF a primit o nouă misiune, aceea de a f uncţiona ca mediu informaţional între Bundesrat şi populaţie.

Această nouă şi complexă misiune a dus la suplimentarea personalului cu aproape 25(X) de oameni. În 1982 a apărut o primă situaţie serioasă, în urma ocupării ambasadei poloneze de la Berna, în această situaţie Bundesrat s-a focalizat pe obţinerea de informaţii din „surse deschise”, acest lucru realizându-l APF.

Ofiţerii APF au sprijinit, de asemenea, între octombrie 1998 şi mai 1999, eforturile ministerului pentru refugiaţi. În acelaşi timp, misiunea principală a APF, aceca de a controla publicarea şi comunicaţiile, a fost menţinută şi pe timp de pace. Starea de pregătire a corpului 4 armată, componentă a gărzii de frontieră ((îrenzwachtkorps) şi a forţelor aeriene a fost testată în 1986. Acest lucru a fost realizat în cadrul unui exerciţiu, de „apărare totală” în eombinaţie cu manevre pe scară largă. Civili, organizaţii civile pentru starea de urgenţă şi

elemente ale transportului public au luat parte la acest exerciţiu.

Aproape 250.000 de persoane din armată şi civili au fost activ implicaţi timp de două săptămâni. APF a trebuit, cu o mie de oameni, să asigure, prin orice mijloace, funcţiunile informaţionale «Ic exerciţiului. Ca scenariu a fost utilizată o stare teoretică de i rizã. Toţi participanţii, ca şi populaţia, au fost confruntaţi cu o mtuaţie imaginară de pericol: sirenele sună şi la radio se anunţa *i* \ există un pericol de radiaţie în urma unui „dezastru enorm în Franţa, nu departe de Basel". Populaţia s-a adăpostit în adăposturi.

Mass-media a încetat, treptat, să funcţioneze. Chiar şi emisiile din străinatate erau foarte slabe. Telefoanele nu mai funcţionau, tu linal, după aproape câteva ore, o voce se aude la radio:, Atenţie! Aceasta este o transmisiune a APF, Departamentul pentru presă ti radio. APF este instrunentul pentru informare al Bundesrat. Aveţi încredere în vocea noastră..."

Transmisiile APF erau foarte puternice şi pătrundeau şi prin betonul adăposturilor. Prin aceasta, dar şi prin alte mijloace, APF a dovedit că poate informa populaţia chiar şi în condiţii foarte dificile. Operaţiunea JNFOSUISSE" a inclus folosirea radioului, televiziunii şi presei. Transmisiunile TV ale APF prezentau de trei ori pe zi programe de 30 de minute în cele trei limbi vorbite în Elveţia.

Pentru aproape cinci zile radiourile APF au transmis pe FM programe toată ziua, acestea incluzând ştiri, anunţuri speciale şi muzică pentru populaţie şi soldaţi. Prezentatorii, femei şi bărbaţi, erau în general cunoscuţi de la televiziunile şi radiourile „normale". Ei erau rezervişti şi au fost activaţi ca membri ai APF. Scopul principal era să se creeze o stare de încredere a populaţiei în persoanele care o informează.

Ţinta finală a acestui exerciţiu, destul de greu de atins pe timp de pace, a fost de a întruni cerinţele psihologice ale actului de informare a populaţiei. Într-o

situaţie reală periculoasă, APF ar trebui să mărească solidaritatea şi dorinţa fiecăruia de a supravieţui, să reducă incertitudinea şi să mărească încrederea în organele de conducere ale ţării.

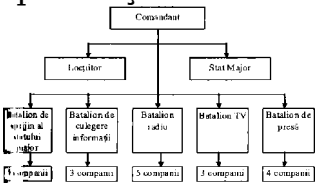
Publicul larg a acceptat radioul şi televiziunea APF. Organizaţiile şi publicaţiile de stânga au fost însă destul de critice, apariţia publică a „mass-mediei de stat", care este planificată să fie utilizată în timpul unei crize informaţionale, nefiind agreată în aceste cercuri. În timpul exerciţiului au fost utilizate staţii radio mobile, televiziunea a operat din locaţii fixe, iar detaşamentele de presă au folosit instalaţii civile (de cele mai multe ori în timpul nopţii). De la acest exerciţiu, APF nu a mai desfăşurat activitaţi într-un mod aşa public şi după câţiva ani s-a reorganizat în regimentul informaţional.

Pentru cazuri speciale, Bundesrat-ul are la dispoziţia sa un comandament separat (Stab Bundesrat, Abteilung Presse und Funkspruch – Stab BR APF) pentru a informa populaţia. Responsabi I pentru acest departament de presă şi radio este tot departamentul de justiţie şi poliţie. Acţiunile acestui comandament se desfăşoară în cazul în care instituţiile civile nu mai sunt în stare (parţial sau lotal) să ducă la îndeplinire sarcinile lor de informare.

Încrederea reprezintă prinicipiul de bază al acestor activităţi. Doar o politică credibilă de informare poate menţine încrederea în conducerea politică şi militară. Informaţia trebuie să fie precisă, relevantă şi pe înţeles. Datorită principiului de încredere pe care îl promovează, acest comandament nu este un instrument de război psihologic.

Comandamentul are un consiliu de conducere al cărui preşedinte este secretarul general al departamentului de justitie şi poliţie. Un organism subordonat (Politisch Publizitsche Leitung – PPL) este responsabil pentru consilierea pe linie de informaţii a guvernului. Regimentul 1 informaţional conduce activităţile massmcdia şi realizează transmisiunile radio şi TV

Regimentul 1 informaţional are structura sa de astăzi începând din 1 ianuarie 1997. Constă dintr-un stat major şi cinci „Abteilunge”, comparabile ca nivel cu batalionul. Unul este pentru sprijinul statului major, iar celelalte (numerotate 10, 20, 30 şi 40) nuni elemente operaţionale. „Input-Abteilung 10” (trei companii) este responsabil pentru obţinerea şi procesarea informaţiilor cu jutorul unor specialişti în limbi străine.



Figură 2. Organizarea regimentului 1 informaţional

„Radio-Abteilung 20” are cinci companii radio care au misiunea de a asigura că guvernul şi comanda militară pot informa rapid populaţia pe întreg cuprinsul ţării. Staţii radio FM foarte puternice, răspândite pe întreg cuprinsul ţării, transmit programe în trei limbi care pot jfi auzite chiar şi în adaposturi de nivel 3. Informaţia poate fi transmisă şi în limbi străine pentru anumite grupuri din ţară sau exterior.

„TV – Abteilung 30” are trei companii TV şi poate sătransmită programe de urgenţă în trei limbi, prin aceasta răspândind mesajele şi directivele autorităţilor regionale şi naţionale.

Companiile radio şi TV pot funcţiona din locaţii subterane amenajate şi dispun şi de staţii mobile.

„Press -Abteilung 40” produce ziare, foi volante şi afişe în cele trei limbi. Aceste produse sâint distribuite din locuri speciale spre populaţie, militari şi unităţile civile pentru starea de urgenţă. Companiile şi detaşamentele utilizează instalaţiile de tipărire de pe întregul Elveţiei. În acest moment, regimentul numără 1640 de militari. Mulţi dintre ei sunt activi în domeniul mass-mediei civile şi toţi au pregătire militară de bază. Viitoarele progrese tehnologice vor putea permite ca numărul personalului să

scadă cu aproape 1000.

Pentru acest regiment, regulile militare din armată nu se aplică în totalitate. În fiecare an ofiţerii şi soldaţii au câteva zile (7 -10) de serviciu activ, tjn soldat poaţe fi în serviciu cel mult 300 de zile şi până la vârsta de 40 de ani. Ofiţerii şi comandanţii pot servi mai multe zile. În cazul unei crize, Bundesrat-ul decide cât personal este necesar. În cazul unei catastrofe, detaşamentele pot fi actiyate imediat pentru unele misiuni speciale.

Pentru transmisii radio, detaşamentele pot fi gata de acţiune în câteva ore. Antrenamentul în vederea misiunilor reale constă din exerciţii de verificare a stării de pregătire după mobilizare în condiţii dificile.

Statul major, elementele de comandă şi „soldaţii mass-media „ sunt pregătiţi în diferite scenarii de criză o dată la doi ani. În 1997, de exemplu, exerciţiul, Alpha" a inclus elemente ale statului major şi „lnput Abteilung 10" Antrenamentul a cuprins „Radio- Abteilung 20", cu două dintre companii, şi „Presse – Abteilung 40", cu elemente din toate cele patru companii.

Exerciţiul a durat 72 de ore şi s-a bazat pe o serie de evoluţii ipotetice în Balcani, „situaţie" în care regimentul trebuie să sprijine mass-media rămasă. Prin utilizarea de noi transmiţători, noi tehnologii şi maşini de tipărit, exerciţiul a dovedit că experienţa şi cunoştinţele de specialitate sunt vitale.

SIGURANŢA INFORMAŢIONALĂ

ERIC LUIIJF M.SC.ENG.[40]

Tehnologia Informaţiei şi Comunicaţiei (ICT-*Information and Comunication Technology*) are un impact imens asupra modului de desfăşurare al operaţiunilor militare. Forţele armate modeme utilizează pe scară largă hardware şi software comercial. Structurile militare şi guvernamentale de luare a deciziei, industriile critice şi societatea în ansamblu devin tot mai mult interconectate în reţele. Ele se bazează pe infrastructuri fundamentale, globale, convergente şi complicate.

40 Laboratorul de fizică-electronică, Olanda.

Cele mai multe din aceste infrastructuri sunt controlate de elemente ICT complexe. Atât sistemele de comandă-control militare precum şi activitatea curentă devine tot mai dependentă de infrastructurile informaţionale.

Siguranţa informaţională, ca parte a operaţiilor informaţionale defensive, are ca obiectiv protejarea atât a posturii de securitate specifkc forţelor armate cât şi a infrastructurilor informaţionale de bază.

Lucrarea abordează aspectele militare şi civile ale siguranţei informaţionale. Ea oferă cititorului o vedere de ansamblu asupra ameninţărilor clare şi prezente specifice cyber-spaţiului pentru foiţele armate şi întreaga societate. Este prezentată o taxonomic a cyber-atacurilor structurate atât după metodele de hacking cât şi după motivul atacului.

Lucrarea discută importanţa ce trebuie acordată siguranţei informaţionale şi concluzionează cu o listă de probleme nerezolvate la nivel internaţional.

Nu cu mult timp în urmă, război 1 în cyber-spatiu, trăgătorii automaţi, muniţia inteligentă şi armele de mare putere energetică au existat numai în literatura de ficţiune şi filme cum ar ti Star Wars (luptătorii stelari).

În zilele noastre operaţiile informaţionale (Info Ops) au trecut de la gândirea conceptuală la realitate şi au devenit un subiect fierbinte atât pentru militari cât şi pentru guverne.

În ultimele două decenii, ICT a avut un impact important în modul de desfăşurare al operaţiunilor militare. În acelaşi timp, 1)cpartamentul Apărării nu mai este factorul principal în evoluţiile din domeniul ICT.

Forţele armate moderne utilizează pe scară largă hardware şi software comercial. De asemenea, structurile militare şi guvernamentale de luare a deciziei, organizaţiile, societatea şi industriile critice devin tot mai mult interconectate în reţele. Pentru funcţiile de bază ele se axează pe infrastructuri globale, convergente, complicate şi adesea publice.

Multe din aceste infrastructuri sunt controlate de sisteme ICT complexe. Atât sistemele militare de comandă-control cât şi tnlreaga societate şi în special „societatea vestică” – au devenit foarte dependente de infrastructura informaţională şi este nevoie de o abordare atentă a ameninţărilor asociate.

Aproape zilnic hackerii explorează vulnerabilităţile Infrastructurilor noastre globale ICT şi ale sistemelor de calcul ilin acestea. Până acum adversarii ideologici şi culturali, cum ar li indivizii, grupurile de guerillă şi grupurile teroriste nu au descoperit complet „războiul informaţional”, ca un mijloc |(îi|lortant de a afecta atât operaţiile militare cât şi societatea.

Distrugerea fizică prin intermediul bombelor şi uciderea Bitrfcenilor prin intermediul atacurilor teroriste reprezintă încă |t jiunile preferate mai mult decât acţiunile în cyber-spatiu. Totuşi, Unole activităţi au identificat deja mijloacele omului sărac de a foto astfel de lucruri. Atât timp cât rămâne ascunsă în a patra îl iii tensiune, infosfera păstrează o distanţă sigură în timp şi spaţiu.

Forţele armate, guvernele şi societatea în ansamblu trebuie să se pregătească pentru a face faţă noilor ameninţări la adresa infrastructurii informaţionale. Totuşi, lipsa curentă de conştientizare despre securitatea informaţională şi vulnerabilităţile infrastructurii informaţionale dau naştere la teama că pericolul clar şi prezent al cyber-ameninţărilor nu este luat în serios.

Siguranţa informaţională, ca parte a operaţiilor informaţionale defensive are ca obiectiv protejarea atât a posturii de securitatea informaţiilor deţinute de forţele armate cât şi a infrastructurilor informaţionale de bază.

Aceasta lucrare abordează atât aspectele militare cât şi civile ale siguranţei informaţionale. Este prezentată o taxonomie a cyberatacurilor şi a atacatorilor şi o viziune introductivă despre hacking şi tehnicile specifice. Lucrarea concluzionează cu o listă de probleme nerezolvate la nivel internaţional.

MC422 al NATO „Politica operaţiilor informaţionale”

defineşte operaţiile informaţionale ca: *Acţiuni desfăşurate pentru a influenţa factorii de decizie în sprijinul îndeplinirii obiectivelor politice şi militare prin afectarea informaţiilor celuilalt, a proceselor bazate pe informaţii, a sistemelor de comandă-control şi a sistemelor de informare şi conducere în acelaşi timp cu exploatarea şi protecţia propriilor informaţii şi/sau sisteme informaţionale*". Există două categorii principale de operaţii informaţionale: defensive şi ofensive, depinzând de natura acţiunilor implicate.

Termenul de „Siguranţă informaţională" a fost introdus de forţele armate ale SUA, pentru a desemna protecţia informaţională a bunurilor proprii şi se defineşte ca: *„Operaţii informaţionale care protejează şi apără informaţia şi sistemele informaţionale prin asigurarea pentru ele a disponibilităţii, integrităţii, autenticităţii, confidenţialităţii şinon-repudieni*". Aceasta include facilităţi de restaurare a sistemelor informaţionale prin încorporarea de capabilităţi de protecţie, detecţie şi reacţie.

Eu văd această definiţie inadecvată din câteva motive. Mai întâi de toate definiţia SUA ia în considerare o listă incompletă de aspecte de securitate informaţională, ea neglijează de exemplu aspectele de securitate, cum sunt credibilitatea, supravieţuirea, siguranţa şi auditul (verificarea de control).

În al doilea rând această definiţie neglijează protecţia infrastructurilor critice şi de bază, care este necesară pentru libertatea politico-militară de a acţiona şi decide. Infrastructurile sunt în zilele noastre globale, îngemănate, şi cel mai adesea controlate de companii comerciale.

Pentru a acoperi toate aceste aspecte, eu propun următoarea definiţie de nivel înalt pentru siguranţa informaţională: *„Siguranţa informaţională reprezintă acţiunile desfăşurate pentru a proteja statul/uniunea, societatea, aliaţii internaţionali, interesele cconomice naţionale şi internaţionale împotriva atacurilor şi* (*listurbanţelor informaţionale din sistemele informaţionale,*

infrastructurile informaţionale, procesele bazate pe informaţii şi infrastructurile informaţionale de bază şi servicii

Definiţia ia în considerare toate capacităţile informaţionale civile şi infrastructurile critice ale unei naţiuni sau ale unei entităţi economice cum ar fi Uniunea Europeană şi aliaţii ei. Desigur, siguranţa informaţională nu poate şi nu ar trebui să se oprească la graniţa ţărilor.

Mai mult, siguranţa informaţională ar trebui să se bazeze pe acordul de sprijin mutual între ţări şi uniuni. Se poate Argümenta că definiţia de mai sus pentru siguranţa informaţională âr trebui să fie „fără stat", ca autostrada informaţională ce traversează multe graniţe de ţări. Statul sau uniunea este cea mai înaltă structură organizaţională care poate trata la nivel ftuţional şi internaţional vulnerabilităţile societăţii informaţionale fn extensia lor, de la dis funcţionalităţi ale serviciilor bazate pe autostrada informaţională la operaţii informaţionale psihologice (Psy Ops).

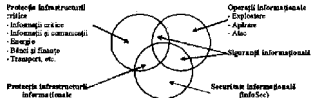


Figura 1: *Legătura dintre siguranţa informaţională, operaţiile informaţionale, securitatea informaţională şi protecţia infrastructurii informaţionale*

Figura 1 evidenţiază legătura dintre siguranţa informaţională, operaţiile informaţionale, securitatea informaţională şi protecţia infrastructurii informaţionale.

În mod curent, forţele armate, structurile guvernamentale şi industriile critice devin tot mai mult interconectate în reţele şi se bazează pe infrastructuri îngemănate şi convergente. Ca un exemplu, peste 95% din comunicaţiile forţelor armate ale SUA pe timpul operaţiei Furtună în Deşert s-au purtat pe linii şi sateliţi închiriaţi.

Cele mai multe dintre aceste infrastructuri informaţionale sunt controlate de elemente ICT complexe. Structurile de bază pentru aceste infrastructuri sunt totuşi

aceleaşi echipamente hardware şi produse software comerciale care sunt utilizate peste tot în lume. Cunoştinţe şi programe despre exploatarea vulnerabilităţilor specifice echipamentelor hardware şi produselor software comerciale pot fi achiziţionate cu uşurinţă. O vulnerabilitate găsită de un hacker seara devreme, în Australia, ar putea să devină cunoştinţe uzuale în alte părţi ale lumii aproape cu viteza luminii. Cu alte cuvinte, sistemele din Europa şi SUA pot fi deja atacate la sfârşitul zilei sau chiar pe timpul nopţii corespunzător timpului local.

Una dintre misiunile forţelor armate ale unei naţiuni este să prevină atacurile posibile la adresa naţiunii şi să apere naţiunea în cazul unui atac al adversarului. Întrebarea este ce rol vor avea forţele armate pentru a realiza apărarea naţiunii în cyber-spatiu. Este nevoie să fie luat în considerare că cyber-spatiu 1 se extinde dincolo de graniţele legale internaţionale şi depăşeşte cu mult spaţiul de luptă militar în dimensiuni de teren, mare şi aer.

Mai mult, în contextul conflictelor militare posibile, există o probabilitate sporită pentru conflicte de tip asimetric şi de intensitate redusă în care operaţiile informaţionale să joace un rol fundamental. Cu toate acestea, ar trebui luat în considerare că ameninţările nu sunt locale unui „teatru” al operaţiilor, dar pot să-şi aibă originea de la oricare adversar oriunde în afara societăţii globale şi pot să se întâmple oricând în cyber-spaţiu.

Cyber-teroristul este o persoană ce acţionează premeditat, o organizaţie non-militară motivată politic, un grup subnaţional, un agent clandestin sau un grup de acţiune sau susţinătorii lor care dispun de posibilitatea unor ameninţări neconvenţionale la adresa unui spectru larg de ţinte militare şi non-militare, inclusiv baza economică.

Într-o perioadă scurtă de timp ei pot genera atacuri împotriva societăţilor din noua generaţie informaţională. Afectarea infrastructurii informaţionale a unei singure naţiuni, de exemplu, membră a unei alianţe ar putea

împiedica, sau chiar opri acţiunile forţelor armate ale întregii alianţe.

Când abordăm latura defensivă, se poate concluziona că forţele armate şi societăţile bazate pe ICT sunt pregătite pentru tratarea noilor ameninţări globale. Deşi tehnologia de informaţii şi comunicaţii de nivel performant este necesară, succesul în atacarea bazelor şi infrastructurilor informaţionale critice nu necesită Investiţii majore şi sunt uşor realizabile de către adversarii potenţiali.

Multe unelte sofisticate şi de ajutor precum şi documentaţia pot fi aduse gratuit de pe Internet, iar şansele de a fi identificat sunt reduse. În concluzie, este necesar un nivel sporit de siguranţă informaţională pentru a face faţă acestor ameninţări.

În ciuda multor semnale de avertisment din partea hacker-ilor, cailor troieni (ex. Back Orifice şi NetBus) căderilor de tensiune şi firelor arse, precum şi conştientizării problemei de tip Y2K, atât forţele armate cât şi societatea erei informaţionale par să nu dorească investigarea şi cercetarea vulnerabilităţilor lor şi să întreprindă în consecinţă măsurile corespunzătoare.

Deşi forţele armate din câteva naţiuni se ocupă de operaţii informaţionale, este adesea trecută cu vederea protecţia bunurilor şi infrastructurilor de management de urgenţă ale guvernului pentru a fi utilizate de către agenţiile guvernamentale şi forţele armate. Cu excepţia unui număr redus de naţiuni, nu este luată în serios continuitatea şi protecţia infrastructurilor informaţionale şi sistemelor informaţionale de bază. Acele naţiuni care întreprind unele acţiuni, înţeleg că ele au de^a face cu o sarcină serioasă care ar trebui să fie îndeplinită în cooperare cu Departamentul Apărării, agenţiile guvernamentale şi prin colaborări publiceprivate. De asemenea, aspectele legale şi regulile existente interzic un curs al acţiunilor „gata de luptă”.

Ca un exemplu, preşedintele Comisiei de Protecţie a Infrastructurii Critice (PCCIP) din SUA are în vedere

vulnerabilităţile din următoarele domenii: informaţii şi comunicaţii, energie (sisteme de tensiune electrică), transport şi stocare de gaze şi petrol, bancar şi financiar, transport fizic (incluzând controlul traficului aerian) şi servicii umane vitale. PCCIP a raportat că există o dependenţă sporită de infrastructurile critice.

Dezvoltările tehnologiei de calcul şi îmbunătăţirile în ritm ameţitor au generat apariţia erei informaţionale şi afectează aproape toate aspectele de comerţ şi societate. Securitatea noastră, economia, modul de viaţă şi poate chiar supravieţuirea sunt acum dependente de acest trio inter-relaţionat al energiei electrice, comunicaţiilor şi calculatoarelor. Inter-legăturile infrastructurilor sunt, pe^uţm spus îngrijorătoare. Oricine prevede ce esté mai rău dacă cel puţin una dintre infrastructuri este afectată, fie deliberat fie ca „voinţă a Domnului”

„CapabiMtăţile de a lansa un atac împotriva infrastructurii informaţionale a unei naţiuni sunt acum foarte răspândite şi un atac probabil nu este foarte departe” avertiza Philip La Combe, preşedintele PCCIP. Afectarea serviciilor de care economia şi bunăstarea noastră depind, ar putea avea efecte semnificative şi dacă se întâmplă frecvent ar putea afecta serios confidenţialitatea publică.

PCCIP a concluzionat că sporirea vulnerabilităţilor cuprinde ameninţările clasice asupra infrastructurilor precum şi noile cyberameninţări. Comanda corect transmisă pe o reţea la un calculator de control al unei staţii de generare a tensiunii electrice ar putea fi comparabilă cu efectul unei încărcături de exploziv. Infractorul ar fi greu de depistat şi reţinut. Mai mult, infrastructurile cresc în complexitate şi sunt operate aproape de capacitatea lor proiectată.

Aceasta sporeşte probabilitatea efectelor în cascadă ce încep chiar cu o distorsiune minoră şi de rutină şi se încheie numai după afectarea unei mari regiuni. Din cauza complexităţii lor tehnice, unele dintre aceste dependenţe nu pot fi cunoscute până când apare o eroare majoră.

Această eroare poate fi introdusă fie de o greşeală operaţională, o eroare tehnică, un act de sabotaj – sau un act de „cybortage”.

Deşi infrastructurile au fost întotdeauna ţinte atractive, naţiunile vecine, prietene şi de graniţă au realizat în trecut elemente de protecţie. Astăzi această situaţie s-a schimbat dramatic deoarece graniţele naţionale nu mai sunt relevante în cyber-spaţiu. Atacurile serioase posibile în cyber-spaţiu pot fi concepute şi planificate firă o pregătire logistică detectabilă.

Ele pot realiza cercetarea invizibil, se pot repeta clandestin, şi apoi pot fi planificate în intervale de minute sau chiar secunde, fără dezvăluirea identităţii şi locaţiei atacatorului. Deoarece Forţele Armate utilizează pe scară largă aceleaşi infrastructuri, devine tot mai dificil să se facă o distincţie între atacuri la adresa forţelor armate şi cele la adresa societăţii.

Aproape zilnic se poate citi în ziare despre exemple de vulnerabilităţi ICT ale societăţii „vestice” şi despre modul cum Forţele Armate şi societatea se ocupă de ele. Oamenii par să zâmbească la aceste incidente şi uită despre impactul care ar putea să apară când sistemele informaţionale şi infrastructura sunt vizate deliberat pe scară largă.

Văzut în această lumină este necesar să revedem câteva exemple.

Lecţiile învăţate din disfuncţionalităţi datorate dezastrelor naturale, de exemplu cutremurul Hansin-Dai-Shinsai, din 17 ianuarie 1995, cu epicentrul aproape de Kobe. Vulnerabilitatea societăţii noastre bazate pe ICT a fost demonstrată în multe moduri. Deşi a existat suficientă hrană disponibilă, ea nu a putut fi vândută deoarece sistemul de comunicaţie ATM a fost afectat cauzând o lipsă de bani lichizi.

Sistemul de comunicaţii de urgenţă de rezervă prin intermediul sateliţilor a fost afectat deoarece cutremurul a deplasat antenele de recepţie la sol şi nimeni din zona de dezastru nu ştia cum să le reahnieze.

Cutremurul din 1995, din zona Golfului San Francisco, a evidenţiat acelaşi tip de vulnerabilitate ICT.

După învăţămintele haosului pieţei financiare cauzat de explozia unei bombe în Piaţa Londrei, pe 4 noiembrie 1992, reprezentanţii IRA au utilizat apeluri anonime pentru a afecta infrastructura serviciilor (ex. zona financiară din Londra). Ei au planificat de asemenea să plaseze fie bombe reale, fie bombe care par a fi reale, la şase substaţii de electricitate din afara „inelului de oţel" de securitate al Londrei.

Dacă planul ar fi avut succes, companiile de deservire implicate ar fi închis ele însele întreaga alimentare cu energie electrică într-un mod controlat. Aceasta pentru a reduce şansele de cădere în cascadă a circuitelor electrice în întregul Regat Unit. A fost estimât că ar fi fost afectate toate serviciile de alimentare cu energie din Londra pentru cel puţin l-l,5 zile. Haosul şi efectele psihologice ar fi fost impresionante. PIRA nu a înţeles (încă) că transmiterea comenzii corecte la elementul de control la distanţă al liniilor de tensiune dă naştere la acelaşi efect.

Fanii fotbalului în încercarea de a obţine bilete pentru Cupa Mondială de fotbal din 1998 au determinat colapsul reţelelor tclefonice în câteva ţări ale Europei, în 22 aprilie 1998. Numai în ( )landa, 30 de oficii telefonice centrale au căzut în câteva ore. Aceasta a inclus patru oraşe importante şi numerele de urgenţă corespunzătoare. La fel ca Rinus Michels, primul antrenor de fotbal, eu am concluzionat *fotbalul reprezintă o infrastructură lie război*

Automatele de vânzare se presupune că apelează compania de distribuţie când devin aproape goale. Totuşi, unele dintre maşinile incorect instalate din Australia au apelat numărul implicit 000, care este numărul de urgenţă din Australia. Deoarece au existăt mii de maşini instalate, aproape 1 milion de apeluri „greşite" pe an au făcut serviciul de urgenţă să blocheze accesul pentru cele ce necesitau intervenţia cu adevărat. Aceste tipuri de „atacuri" larg răspândite par să fie greu de gestionat.

Pe 10 martie 1997, un hacker tânăr a închis comutatorul oficiului central al companiei Bell Atlantic din Worcester aproape de Boston, SUA. Ca rezultat aeroportul a pierdut serviciile tclefonice şi de date pentru mai bine de 6 ore. Pe 4 ianuarie 1999, cinci indivizi au pătruns într-un oficiu telefonic din Las Vegas Sprint şi au oprit echipamentele de comutare telefonică. Aceasta H determinat 7 ore de întrerupere a serviciului telefonic pentru 75.000 de clienţi.

Pe 19 mai 1997, satelitul PanAmSat Galaxy IV a fost scăpat de sub control, întrerupând serviciul de pager pe perioada a 3 fi pentru 80-90% din 40 de milioane de pagere utilizate în SUA. L>octorii au fost printre primii afectaţi, deoarece spitalele le făceau Ipeltni în caz de urgenţă, precum şi ofiţerii de poliţie.

Amsterdam Internet Exchange a căzut pe 26 decembrie 1998 lia tontă unei defecţiuni a transformatorului de tensiune electrică. Dltinda a fost efectiv tăiată de la Internet pentru un număr de ore. *K lé* iunie 1999,4 fire au fost tăiate la Groningen, determinând D « oprire instantanee a serviciilor mobile şi fixe precum şi pierderea în viciilor de date în provinciile nordice ale Olandei.

Pe 26 martie 1999, macro-viermele Melissa s-a răspândit foarte rapid pe Internet. Multe site-uri guvernamentale ale SUA incluzând baza militară ce susţinea operaţia din Kosovo au apărut a fi vulnerabile. Din fericire, viermele nu a avut „efecte44 distructive.

Din aceste cauze şi multe altele, din faptul că aproape zilnic se înregistrează incidente grave ar trebui să fie clar că forţele armate, guvernul, societatea, organizaţiile şi industriile critice trebuie să se pregătească împreună pentru apărarea bunurilor lor în era informaţională.

Cyber+atacurile şi cyber-terorismul pot fi găsite pe harta rutieră specifică operaţiilor informaţionale. Întrebarea este dacă cineva ar putea privi asta ca o ameninţare a viitorului, o ameninţare futuristă sau ca o

ameninţare a zilelor noastre. Este ea reală sau este ficţiune? În studierea acestei probleme, bazele de informaţii deschise nu prea oferă fapte substanţiale.

De exemplu, infracţiunile în domeniul calculatoarelor nu sunt înregistrate ca un element distinct de către cele mai multe birouri de statistică. Ele vor fi probabil clasificate drept infracţiuni cum ar fi furtul, falsificarea sau altă categorie. Astfel nicio abordare sociologică a cyber-atacurilor nu este la îndemână. Infractorii se află de la copii de şcoală, studenţi, oameni bolnavi mintal care trăiesc izolaţi de societate până la terorişti reali.

Unele grupuri de hackeri ex. *Master ofDownloading* (MOD) au membri multinaţionali. Pe de altă parte, terorismul însuşi va rămâne o problemă trans-naţională, condusă de minoritatea etnică, religioasă, naţionalistă, separatistă, politică şi motivaţii economice. Cyber-terorismul este gata să apară în toată măreţia lui cât de curând. Pentru a răspunde întrebării „*Cyber-atacul*: *fapt sau ficţiune*?” trebuie să facem o evaluare în vederea clasificării diferitelor aspecte legate de acestea.

Când sunt evaluate diferite tipuri de conflicte care ar putea să apară, ar trebui avut în vedere tipul şi intenţia adversarilor potenţiali. Tabelul I, potrivit lui Waltz furnizează o astfel do abordare.

Rizbuiic *de* goenE

	Nivel tehnic ridicat

	Conflict fizic	1. Război camandăoontrol – câmp de luptă de în intensitate -presiune şi p economică -ţinta: precis consecinţa: fizică -tehnologia
Războaie pe baze economice	Conflict abstract	2 Război în ieţde, c războ – conflictul în cyber-sp cunoştinţe şi putere -ţinta: de informaţii -conse utilizarea ITC – reţele glob tehnologice

Războaie culturale

Tabelul 1. Tipologia a patru tipuri de conßict

Este clar că accentul important în dreptunghiul 1 revine componentei militare (operaţii informaţionale; războiul de comandă-control). Cyber-teroristul de înalt nivel tehnic (dreptunghiul

2 în figură) – un individ premeditat, o organizaţie militară motivată politic, un grup sub-naţional, un agent clandestin, sau un grup de acţiune – sau suporterii lor care au posibilitatea generării unor ameninţări neconvenţionale la adresa unui spectru larg de ţinte militare şi ne-militare, incluzând baza economică.

Un avantaj major pentru protagonistul virtual (dreptunghiul

3 şi 4) este că acesta nu este nevoie să se găsească în preajma, în timp sau spaţial când se realizează atacul sistemului sau infrastructurii. Pregătirea unui atac întârziat este uşoară deoarece modemul de comunicare pentru lansarea atacului poate fi uşor programat automat.

Infrastructura globală face uşoară alegerea unei ţări din care atacul este pregătit şi la fel este uşor de ascuns utilizarea liniilor telefonice internaţionale pentru a ajunge la un modem în altă ţară. Pentru securitatea serviciilor, guvernului şi organizaţiilor atacate le va fi greu să aibă indicii asupra ţintelor care ar trebui selectate. Lipsind această informaţie, va fi greu de găsit timpul necesar avertizării. Urmărirea şi indentificarea grupurilor teroriste virtuale va fi chiar dificilă dacă nu imposibilă.

Posibilitatea de a utiliza aceste aspecte ca mijloace tehnice, utilizând tehnologii noi şi combinate, face situaţia diferită în raport cu mijloacele de război existente înainte. Costul relativ redus, rata de succes posibil ridicată şi probabilitatea de a o deţine, fac în principiu „Operaţiile informaţionale ofensive” atractive pentru indivizi, adversari economici, precum şi pentru grupurile de protest şi teroriste.

Prima abordare este de a vedea tipurile de preocupări de hacking în cadrul tabloului general de hacking.

— Hackeri – cei ce vor să pătrundă fraudulos pentru a demonstra vulnerabilitatea sistemelor de calcul şi a reţelelor prin exploatarea sistemelor administrate „mai puţin bine” şi/sau a punctelor slabe cunoscute. Intenţia lor nu este de cele mai multe ori una distructivă, dar generează o întrebare de genul „Ce va fi dacă...?” Acestea includ strănuturi şi sughiţuri la adresa celor ce ascultă pe reţele pentru parole simple.

Crackeri – cei ce pătrund în sistemele de calcul, încercând să distrugă sau să modifice informaţii sau să exploateze aceste sisteme ex. distribuirea ilegală de

software. Crackerii software sunt specialişti în acest grup care sparg verificările de securitate/ identitate ale pachetelor software.

Phreakeri (anomalii telefonice), expoatează schimburile telefonice, sistemul telefonic celular şi utilizarea semnalului telefonic pentru fraudă. Ei, de asemenea, pot fi implicaţi în frauda de cartele inteligente şi cărţi de credit. Grupul phreak-erilor „Specialiştii în telefoane" au pătruns la comutatoarele AT&T, Southern Bell, BT, au avut acces la porţiuni din reţeaua de electricitate a SUA şi la sistemele de control a traficului aerian. Ei au redirecţionat liniile telefonice ale FBI înspre liniile telefonice pentru discuţii de sex din Germania şi alte ţări şi au obţinut acces la listele de linii telefonice ascultate (în final a reieşit că însăşi liniile lor telefonice erau monitorizate de FBI).

Socio-ingineri, cei ce sunt culegători de informaţie de nemulţumire, ceea ce le permite să culeagă parole sau alte informaţii vitale pentru a accesa sistemele şi reţelele. Thrash-erii (bităuşi) sunt socio-ingineri ce utilizează metode de culegere fizică a informaţiilor. Aşa numiţii dumpster-divers (scafandrii în gunoaie) care umblă prin gunoaiele companiei pentru a găsi Informaţii valoroase ce pot să-i ajute să pregătească un atac socio- Ingineresc sau să atace direct.

Hackeri pentru modemuri de cablu TV, comunicare prin Satelit şi de plătire a taxelor TV, sunt cei care sparg sistemul de Codificare al semnalului TV în scopul de a vedea transmisiunile gratuit. Acţiunile lor curente au numai impact economic. Prin oferirea posibilităţii de acces Internet prin intermediul modemurilor de cablu CATV, ameninţările la adresa confidenţialităţii, integrităţii şi securităţii devin o problemă. Totuşi acestea sunt clasificate în alte categorii.

VX, creatori de viruşi, indivizi ce scriu programe virus şi le lansează în acţiune. Aşa numiţii „*lamers*" sunt de clasă mai slabă „ei utilizează chituri de construcţie pentru yiruşi, fac mici modificări nefolositoare sau doar infectează

calculatoarele altora...

Screen droppers (culegători de ecran), monitorizează de la distanţă, pe ascuns, ecranele calculatoarelor utilizând radiaţia electromagnetică a ecranelor. Aceste sisteme ar putea culege informaţia de pe ecran de la o distanţă de 1 km. Măsurătorile cu Standardul de Emanaţie a Pulsului Electromagnetic Tranzient (TEMPEST) reduc considerabil expunerea la acest risc.

Utilizatorul intern: poate fi oricare dintre cei de mai sus care poate avea acces „nelimitat" la informaţia şi sistemele interne.

În al doilea rând am putea ordona cyber-aţacurile pe baza motivelor atacurilor şi în funcţie de cine este în spatele acestor atribuţuni.

Incompetenţa, neglijenţă. *Subiectul*: utilizatorul intern. *Scopul*: evident fără scop. De observat că tot ce a fost spus despre hack-erul extern ar trebui pus în balanţă cu rezultatele mai multor studii ce arată că utilizatorul intern este responsabil pentru 60%- 80% dintre breşele existente în securitatea informaţiei. Lipsa de apărare datorată neglijenţei şi lipsa de conştientizare a securităţii este cauza principală a atacurilor cu succes. Cei din afară pot ataca adesea prin utilizàreà căilor lăsate neblocate de către administratorii de sistem şi dé reţea. Mai mult, orice organizaţie ia măsuri importante pentru a determina activităţile neautorizate ale utilizatorilor interni.

Interzicerea (refuzul) intern de serviciu. *Subiectul*: angajatul nemulţumit care vrea să-şi răneasscă şeful *Scopul*: resturi arse (informaţii şterse sau stricate) sau informaţii blocate (chciu cunoscută numai de şef).

Haclring de recreaţie/amator. *Subiectul*: Un singur individ sau un grup restrâns de adolescenţi, studenţi şi persoane interesate tehnologic, uneori lucrând în grupuri similare (egale). *Scopul*: Încercarea de a înţelege ICT şi calea prin care uneori sau adesea sistemele de securitate nu funcţionează (curiozitate). *Riscul limită*: persoana poate deveni un „mic criminal" prin obţinerea de Rezultate financiare (ex. phreaking, fraudă de cartele inteligente).

Nesupunere electronică. *Subiectul*: grupuri de activitate, Suporterii unei cauze. *Scop*: obţinerea atenţiei mijloacelor de informare şi întreruperi temporare ale serviciilor prin atacuri de interzicere a serviciului. *Riscul limită*: să devină mai violent când acţiunile nu au impactul scontat. De exemplu: Teatrul de Disturbanţă Electronic în sprijinul mexicanului Zapatista a invadat scrverele web ale preşedintelui mexican, Biroul de Schimb al Stocurilor din Frankfurt şi Departamentul Apărării al SUA cu cereri de pagini web. Rezultatul a fost interzicerea serviciului pentru ceilalţi utilizatori.

Hacking pentru căutare de publicitate. *Subiectul*: Un singur individ sau un grup restrâns de adolescenţi, studenţi şi persoane Interesate tehnologic precum şi un grup de hackeri (semi) profesionali. *Scopul*: intenţia de a obţine o atenţie sporită în mijloacele de informare prin pătrunderea într-un sistem ICT Important şi comentarea acestui fapt. *Riscul limită*: să devină Implicaţi/angajaţi de criminali sau grupuri sub-naţionale.

Căutător de suport legal. *Subiectul*: Persoana sau grup de hucking semi-profesional; angajat nemulţumit de şeful „direct”. *fii opul*: Încercarea de a discredita un serviciu ICT şi/ sau serviciu llv deservire, pentru a-şi dovedi propria inocenţă. *Riscul limită*: a llrveni „violent” încercând să impună propriul punct de vedere.

Obţinerea de informaţii. *Subiectul*: Comunităţile de JflkiHigence naţionale, culegătorii de informaţii economice (firmele di) intelligence în afaceri), spionaj economic şi industrial şi purlOane/ grupuri profesionale de hacking. *Scopul*: serviciile de informaţii naţionale şi de afaceri, pentru a obţine un avantaj faţă de alte naţiuni şi organizaţii.

Grupuri de acţiune pentru o cauză; protagonişti criminali („hack-ivişti”). *Subiectul*: Orice grup motivat cu cunoştinţe sau pregătire tehnologică. *Scop*: căutarea de publicitate şi încercarea de a enerva organizaţia, departamentul guvernamental sau agenţia în discuţie. *Mijloace*: urmărirea de atacuri de interzicere a serviciului

ex. prin depăşiri de memorie, precum şi pierderea de integritate a sistemelor. *Riscul limită*: a deveni „violent” în încercarea de a face cunoscut punctul lor de vedere şi deplasarea înspre terorism.

Ca un exemplu, în august 1999, câştigătorul premiului NOBEL pentru pace din 1996, Jose Ramos-Horta a ameninţai guvernul indonezian. Un grup de peste 100 de hackeri din întreaga lume au simpatizat cu luptătorii pentru indtependenţă din Timonil de Est şi erau gata să atace bunurile economice principale ale Indoneziei (bănci, operatori de telecomunicaţii, linii aeriene), în caz că guvernu 1 indonezian nu accepta rezultatele referendumului ţinut în Timonil de Est.

Avantaj economic. *Subiectul*: Un partener de afaceri fără scrupule sau un angajat „flexibil etic”. *Scopul*; obţinerea de beneficii prin afectarea activităţilor de ICT ale competitorilor.

Vandalism. *Subiectul*: În principal angajaţii sau indivizii nemulţumiţi. *Scopul*: Atingerea valorilor economice ale unei organizaţii.

Activităţi criminale. *Subiectul*: Persoane/ grupuri do hacking profesionale având ele însele scopuri criminale sau angajate de criminali sau grupuri criminale. *Scopul*: Activitate« (dacă e posibil ascunsă) de a obţine informaţii, contra-informaţii (ex. Obţinerea, distrugerea, discreditarea informaţiilor poliţiei) pentru a afecta securitatea infrastructurilor pe timpul unei acţiuni planificate sau pentru a obţine un avantaj financiar.

Cyber-terorism. *Subiectul*: Grup sub-naţional premediUil, motivat politic, agent clandestin, grupuri criminale organizate sau concurenţi economici fără scrupule. Ar putea utiliza grupuri sau persoane de hacking profesional plătite. Dacă atacul este străin sau din interior nu se realizează nicio diferenţă. *Scopul*: Un spectru larg de ţinte militare şi ne-militare incluzând baza economică.

De reţinut din cyber-atacuri că noile mijloace ICT în general şi Internet-ul în particular, sunt utilizate ca mijloace de comunicare pentru distribuirea informaţiilor

sub-naţionale, teroriste şi Criminale (ex. recipiente bombă, curse de prindere prin blocare, Oferte de paşapoarte ilegale) şi comunicarea secretă. Aceste categorii nu sunt tratate în această lucrare.

Pe lângă erorile generate către utilizatorul intern, cele mai multe cyber-atacuri au propriile lor circuite informaţionale subterane (ascunse), uneori chiar în bazele de informaţii deschise pe web. De exemplu, instrumente phreaker şi cunoştinte sunt utilizate pentru a deschide un circuit telefonic.

Hackerii ar putea să treacă prin sisteme de calcul multiple şi Nil se schimbe înainte de a ajunge la ţinta lor care ar putea să reprezinte mersul prin ţări diferite. Unele grupuri de hacking sunt hi ne organizate şi au propriile lor publicaţii (ex. 2600 în SUA, un e a apărut de mai bine de 10 ani, Clubul Haosului Calculator în Ucrmania). Multe articole pe acest subiect pot fi găsite de nimenea pe WWW.

Hackerii/phreakerii interschimbă documente cu cunoştinţele lor îli care se găsesc chiar elemente de proiectare hardware. Uneori Humagerii de sisteme Unix şi Windows/NT cunoscători, utilizează li-este surse pentru obţinerea de detalii de profunzime. Cele mai piuite documente şi baze de date care au deinformaţii referitoare vulnerabilităţile unui sistem pot fi găsite pe Web.

Separat de atacurile fizice, diferite tipuri de mijloace de atac Itilnfmaţional variază de la un mod de atac strict software la ttM|loace în spectrul electro-magnetic. O listă exemplu a acestor Ini | loace este prezentată mai jos.

Virus calculator: cod care seauto-reproduce când este executat şi infectează pe ascuns codul executabil, incluzând macrocodul. Separat de codul reprodus, un virus conţine o taxă de încărcare care se poate manifesta prietenos sau distructiv. Viruşii sunt secvenţe de program nedirijate. Viteza lor de infectare depinde de tipul mecanismului de infectare utilizat. Cu toate că uneori sunt distructivi sau enervanţi, viruşii sunt cele mai puţin utilizate mijloace pentru operaţiile informaţionale.

Cal troian: cod ce are ascuns efecte laterale. Web-

site-urilc bune şi frumoase cu cod activ (Java, ActiveX) reprezintă un pericol pentru descărcarea acestui cod sau vizitarea unor astfel de site-uri.

Vierme: cod auto-replicat (multiplicat) ce utilizează funcţionalitatea reţelei ex. mecanismele de distribuţie e-mail, pentru a se împrăştia. Virusul „Melissa” care s-a împrăştiat aproape instantaneu pe Internet în 1999, a fost un astfel de vierme.

Bomba logică şi bomba cu ceas: o porţiune ascunsă de cod care se execută când o condiţie certă-filtrată extern ex. timp, ştergerea unui fişier, schimbarea unui web-site extern se realizează.

Torpedo logic: un tip de virus ce încearcă să avanseze cătrc o mulţime de scopuri certe (sigure), având un sistem sau un program pentru livrarea consecinţelor sale acolo.

Manipularea datelor: variază de la discreditarea integrităţ i i informaţiei la schimbarea biţilor datelor la video-morfologie în care informaţia video sau chiar imaginea este manipulată într-un asemenea mod că de exemplu un preşedinte strânge mâna cuiva pe care nu l-a întâlnit în întreaga viaţă.

Uşa din spate sau uşa trapă: o portiţă în sistem lăsată de programator sau administratorul de sistem permiţând utilizatorilor neautorizaţi să obţină accesul la o parte sau la întreg sistemul.

Proiectarea sistem şi sisteme de codificare: pentru fiecarc sistem de operare, software reţea, elemente de comutare reţea şi echipamente de protecţie de graniţă (ziduri de foc, gărzi) listele cu vulnerabilităţi şi petece sunt publicate de vânzători şi Echipe k de Răspuns de Urgenţă pentru Calculatoare. De obicei administratorii de sistem nu dispun sau au timp limitat pentru a instala programe petec, în măsura în care această informaţie dispare. Aceasta are ca rezultat existenţa portiţelor deschise, binecunoscute pentru multe sisteme de producţie.

Depăşirea de memorie: bombardarea unui sistem cu foarte multe cereri aşa încât sistemul nu poate face faţă fluxului de intrare rezultând un refuz al serviciului pentru

utilizatorii autorizaţi. O unealtă soft ce a fost proiectată pentru situatii de, jnundaţii" este numită *FloodNet* şi este produsă de Teatrul de Disturbanţă Electronic.

Proiectarea circuitelor: modificarea circuitelor într-un astfel de mod în care circuitul (chipul) conţine o uşă prin spate sau o bombă logică.

Cutii albastre: pătrunderea pe linii telefonice şi „jocul" cu semnalele electronice.

Apelator de război: O setare software şi de comunicare (modem) ce permite apelarea secvenţială rapidă a listelor de numere de telefoane în scopul de a detecta modem-uri active sau linii telefonice ce permit „dialogul-după".

Mijloace în spectrul electro-magnetic, unele exemple:

— Înregistrarea informaţiei utilizând radiaţia ecranelor şi softul TEMPEST (soft pentru emisii stimulate).

— interferarea cu semnale radio, ex. un sistem de supervizare ÜSM, precum şi cu transmiţătorii de mare putere în spectrul de bandă ultra-largă.

— pulsuri electromagnetice, încărcarea şi chiar distrugerea circuitelor sistem;

— echipamente bazate pe micro-unde de mare putere.

Pentru a evidenţia ameninţările cyber-atacurilor, tabelul de mai jos dă o estimare a probabilităţii ţintei prin ţintă şi motiv. În acelaşi timp se arată dacă atacurile validate au fost raportate de către sursele deschise.

CYBER-ATACURI	Atacun validate (Septembrie 1999)	TINTE *9*	
		Informaţia	Sis & Reţele

Incopetenţă, neglijenţă	Larg răspândit	Ţintă principală	Ţin principal
Refuzul intern al serviciului	Laig răspândit	Ţintă J principal ă	Lin
Hacking de recreere	Larg răspândit	Limitat	Ţin principal
Nesupunere electronică	Limitat		Ţin
Hacking în căutare de publicitate	Larg răspândit	’ţintă principală	Lin
Căutător de suport legal	Limitat	lină principală	

Obţinerea dfc informaţii econamce	Li ni tat, în creştere rapidă	Ţint ă principală			
Atac/ rezultat economic	limitat, în creştere rapidă	Ţint ă principală	Ţint ă principală	Ţint ă principală	
Obţinerea de infoimaţii naţionale	Cunosc ut că se întâmplă	Ţint ă principală		Limi tat?	tă?
Grup de acţiune /hackivist	Limitat, în creştere	Limi tat	Ţint ă principală	Ţint ă principală	tă pri ă
Vandalism	Limitat		Ţint ă	Ţint ă	tă

			principală		
Criminali: crimă simplă	limitat	Ţintă principală		Ţintă >	
Criminali: crimă financiară	La nivel înalt, în creştere rapidă	Ţintă principală	Phreak-ing	Ţintă	
Crimă organizată	Necunoscut	Ţintă principală		Ţintă principală	tă
Cyber-terorism	PIRA: limitat				tă
	limitat	Ţintă principală	Ţintă	Ţintă	tă

Personalului de întreţinere din spaţiul SUA şi Centrul de Război al Sistemelor Navale din San Diego i-a fost cerut să investigheze plângerile utilizatorilor privind imprimarea cu viteză redusă. Hackerii au redirecţionat fluxul de imprimare la un server în Rusia, care în final întorcea ieşirea la imprimanta de destinaţie. Se poate intui ce se putea întâmpla cu rezultatul imprimării.

Pe timpul crizei diţi Kosovo, au fost raportate din surse ca Serbia şi Rusia precum şi de la simpatizanţi din alte ţări ^tacuri la adresa sistemelor NATO, sistemelor guvernamentale ale SUA şi sistemelor de apărare ale partenerilor coaliţiei. Separat de atacurile de interzicere a serviciului şi de dezafectare a site-urilor web au fost făcute încercări de a pătrunde în reţelele apărării.

Astfel, când se discută problema „Cyber-atacuri: fapt sau ficţiune” putem concluziona că toate tipurile de cyber-ameninţări au fost realizate într-un mod sau altul. Zilnic, se pot găsi articole în ştirile despre sisteme afectate, cărţi de credit şi infrastructuri afectate. Totuşi, atacuri la întreaga scară, cu un impact major asupra forţelor armate

şi/sau societăţii nu au fost (încă) realizate.

Infrastructurile informaţionale sunt dependente de ICT, îngemănate şi inter-relaţionate. Ele sunt foarte vulnerabile. Înjur de 80% până la 90% din informaţia necesară pentru apărarea unei naţiuni este în zilele noastre deţinută de sectorul privat, cu alte cuvinte este în afara controlului guvernamental. Sunt necesare schimbări fundamentale în abordarea siguranţei informaţionale în societatea secolului XXI. În continuare sunt evidenţiate unele dintre problemele deschise.

Organizaţiile în general nu acordă suficienţă atenţie securităţii informaţionale, neglijează avertismentele, nu pot păstra evidenţa modificărilor semnificative în cadrul mediului reţea şi sunt nepregătite pentru lucrurile care ar putea să se întâmple. Sunt chiar convins că multe agenţii guvernamentale au sisteme senzitive şi reţele ce posedă porţi neblocate care aşteaptă să fie deschise de către neautorizaţi.

Industria de obţinere a informaţiilor electronice economice, atât etică cât şi neetică, se extinde rapid. Există indicatori că obţinerea avantajelor financiare prin utilizarea atacurilor economice ne-etice este în creştere, oferind o şansă redusă de detectare. Cât timp va accepta societatea aceste riscuri?

Cele mai multe guverne au deficienţe cu conştientizarea vulnerabilităţii propriilor lor societăţi. Manifestarea internaţională a cyber-terorismului poate fi aşteptată mai devreme sau mai târziu. Studii precum cele ale PCCIP al SUA nu sunt încă realizate în cele mai multe ţări sau sunt împiedicate de lipsa de cooperare cu alte agenţii şi industrii guvernamentale.

În cyber-spaţiu cineva poate ataca fie de peste stradă, fie de undeva din Timbuktu, fapt ce face şi mai dificil mersul după cyberatacatori. Singura soluţie este păstrarea permanentă a porţilor închise, ceea ce înseamnă vigilenţă continuă. Organizaţiile care utilizează pe scară largă mijloace de informaţii şi comunicaţii, cum ar fi forţele armate, au resurse foarte limitate atât în termeni

de calitate (cunoştinţe) cât şi cantitate (numărul managerilor de sistem).

Este deja dificil de a ţine infrastructura informaţională în funcţiune pe o bază de zi-cu-zi. Resursele pentru menţinerea posturii de securitate sunt nesatisfacătoare. Organizaţiile ar trebui tiă devină conştiente că siguranţa informaţională ar trebui să se alle pe lista lor de priorităţi în scopul de a supravieţui operaţiilor informaţionale ale adversarului. Problema este dacă acţiunile vor li întreprinse la timp sau va trebui să avem experienţa unui „Pearl Harbor electronic".

Pentru soluţionarea acestor robleme este necesar un efort legal internaţional fundamental de abordare a vulnerabilităţilor din |cyber-spaţiu, un cadru legal internaţional, cooperarea poliţiei Jinlprnaţionale, definirea legală a cyber-atacului şi a tipurilor de Âpărări permise împotriva operaţiilor informaţionale. În mod turent, suportul legal internaţional este ineficient datorită procedurilor complexe.

| Adversarul pe de altă parte are nevoie numai de secvenţe IcUrte de biţi care sunt măsurate în secunde. În al doilea rând, pregătirea actuală a poliţiei implică criminali nu terorişti. Cine va apăra ţările împotriva cyber-terorismului? Care va fi rolul serviciilor de securitate în secolul XXI, date fiind ameninţările de cyber-terorism şi terorism la adresa infrastructurilor? Cum ar trebui să fie organizat schimbul de informaţie intern al statului pentru a lupta împotriva ameninţărilor ce traversează graniţa?

Pregatirea de urgenţă necesită instruirea şi reevaluarea. Siguranţa informaţională impune forţelor armate, guvernelor şi furnizorilor de infrastructuri critice de informaţii să fie pregătiţi pentru administrarea protectivă a acţiunilor în cazul unui atac. Întrebarea este cum să se dezvolte scenarii de reevaluare realiste, considerând în particular aspectele de depăşire a graniţelor specifice cyber-spaţiului.

Tot mai mult, forţele armate şi agenţiile guvernamentale utilizează activ echipe „Tiger" sau echipe

de infiltrare pentru a încerca să pătrundă în propriile lor sisteme senzitive. Există un număr de aspecte legale când se lansează aceste aşa numite capabilităţi de „Echipă Roşie” care este nevoie să fie rezolvate.

Practic siguranţa informaţională necesită căutarea activă de găuri în apărarea cuiva în combinaţie cu detectarea intruşilor şi instruirea echipelor de răspuns. Când privim aspectele internaţionale întrebarea este dacă ţările ar trebui să coopereze în activităţile Echipelor Roşii la nivel tehnic. Este necesară o evaluare continuă a infrastructurilor informaţionale internaţionale.

Există o scăpare curentă a atenţiei managementului pentru conştientizarea securităţii informaţionale. Întrebarea este cum să înceapă conştientizarea de siguranţă informaţională de la nivelul corect în Forţele Armate şi organizaţiile guvernamentale.

O soluţie simplă la unele dintre problemele siguranţei informaţionale este să se interzică toate comunicaţiile electronico şi schimburile de informaţii. Pe de altă parte există presiune pentru utilizarea în comun a informaţiilor internaţionale între coaliţii partenere şi guverne. Cum să se păstreze confidenţialitatea, integritatea şi disponibilitatea informaţiei cuiva dacă un grad sigur de schimb este necesar înainte de obţinerea de informaţii din alte părţi? Pentru a opera cu această dilemă, sunt necesare dezvoltări pe mai departe ale siguranţei informaţionale.

Şi la final, dar nu cea din urmă, hacking-ul şi phreaking-ul reprezintă o realitate. Totuşi cei mai mulţi dintre ei sunt hackeri de recreaţie. Întrebarea este ce unelte de alertare ar trebui dezvoltate pentru a recunoaşte „posibilii” spioni, criminali şi terorişti în ansambluţ zgomotului de fundal.

CONCLUZII

Pentru a supravieţui posibilelor cyber-atacuri din partea teroriştilor virtuali, fie pentru motive ideologice, fie pentru alte motive, este nevoie ca ţările, guvernele şi organizaţiile să fie pregătite. Cyber-atacatorul are

avantajul de a fi plasat în timp şi spaţiu independent de ţintă, în timp ce tehnologia necesară este relativ ieftin de obţinut.

Siguranţa informaţională se presupune că este răspunsul la ameninţarea asimetrică. Din acest motiv, siguranţa informaţională care include aspecte de securitatea informaţiilor, protecţia infrastructurii de informaţii şi operaţii informaţionale defensive, necesită mai multă atenţie decât le este acordată în prezent. Lipsa de conştientizare, de management de securitate şi analiza corespunzătoare a riscurilor generează mari riscuri neconsiderate.

Utilizarea echipamentelor hardware şi software comerciale sporeşte vulnerabilităţile posibile ale sistemelor şi infrastructurilor hi situaţia în care exploatarea vulnerabilităţilor cunoscute nu sunt înregistrate imediat. Producătorii comerciali nu sunt doritori să adauge mecanisme ce permit siguranţa informaţională şi încrederea. Întrebarea este cum să se menţină încrederea când se Utilizează predominant componente comerciale.

Şi deoarece lumea ICT (virtuală), conectivitatea globală, infrastructurile convergente şi reţelele interconectate traversează (tiuite graniţe internaţionale, cooperarea internaţională efectivă Va fi esenţială pentru a înregistra atacurile la adresa naţiunii sau Infrastructurii informaţionale de apărare.

Faptul că forţele armate şi comunicaţiile de management de urgenţă se bazează parţial sau uneori chiar în mare măsură, până la o treime deţinută de infrastructurile civile, reprezintă o mare problemă. Cooperarea internaţională se bazează încă pe tehnologia antică cu factori poştali şi procedurile administrative sunt lungi dacă nu chiar birocratice.

Cyber-atacatorul, pe de altă parte utilizează autostrada electronică cu viteza luminii şi este informai organizat. Este încă un drum lung de parcurs pentru a acoperi golul pe care îl reprezintă siguranţa

informaţională. Aceasta necesită atât sporirea conştientizării la cele mai înalte nivele de luare a deciziei, dezvoltări tehnologice majore şi cooperarea globală pentru sisteme legale armonizate şi suport pentru investigarea criminalităţii.

EXPLOZIA TEHNOLOGIEI INFORMAŢIEI

MAX V. METSELAAR*

Este acceptat astăzi că aplicaţiile noilor tehnologii ale în formaţiei au un impact semnificativ asupra managementului conflictelor şi crizelor şi acest impact este de aşteptat să crească în viitorul apropiat. Acest articol examinează câteva avantaje şi dezavantaje ale dezvoltării acestor tehnologii în ceea ce priveşte Icnientele cheie ale managementului conflictelor şi crizelor: Importanţa de a fi cât mai pregătit posibil şi anticiparea încercărilor Id versarului de a desfăşura un atac surpriză. ’ în ce fel şi la ce scară aplicarea, prin intermediul atacurilor iu îi actelor teroriste, a tehnologiilor moderne ale informaţiei poate lluce la degradări ale stării de pregătire? Pe baza rezultatelor studiilor desfăşurate în ultimele decenii în cadrul diverselor discipline, va rezulta concluzia că introducerea tehnologiei llilonmaţiei generează atât avantaje, cât şi dezavantaje.

În multe privinţe, această introducere apare a fi ceva în genul lipului lui Janus”: pe de o parte ajută potenţialul apărător de a-şi Ipori capacităţile de intelligence, diseminarea pe verticală şi pe Uiizontală de intelligence, în cadrul segmentelor sistemelor C4I |l i ciclurilor de luare a deciziilor, poate deveni mai rapidă ca llicând. Pe de altă parte, trebuie să se ţină cont de multe On|ayantaje şi capcane periculoase ce pot apare.

Re lângă creşterea semnificativă a capacităţilor apărătorului fti u obţine, analiza, verifica şi disemina diferite tipuri de IHfcltigence despre intenţii şi tipuri de ameninţare, va duce şi la

Academia Militară Regală, Breda, Olanda creştea cantităţii de informaţii irelevante. Mai departe, introducerea tehnologiei informaţiei ar putea conduce la

apariţia unor erori în ceea ce priveşte controlul situaţiei şi avertizarea.

O privire asupra documentelor despre războiul din Golf din 1991 şi războiul din Kosovo din 1999, precum şi asupra conferinţelor, publicaţiilor şi filmelor promoţionale despre războiul viitorului, sugerează, datorită comentariilor militarilor şi oamenilor de ştiinţă, că era informaţională aduce doar beneficii.

De exemplu, remarci ca „gândiţi-vă la ceea ar însemna să.îi la dispoziţie posibilităţi de supraveghere a unui câmp de 200 de mile şi să fii în stare să trimiţi rachete balistice oriunde pe câmp în doar patru minute – o rachetă care merge precis exact undo vrei” sau „sistemul C3I global va fi arma principală a secolului XXI”, indică faptul că apariţia progreselor tehnologiei informat irl în domeniul sistemelor C4I (command, coordination, contml, comunication and intelligence) aduce beneficii calităţii şi eficienloi operaţiunilor viitorului. Trebuie, însă, să se pună întrebarea dac é un asemenea optimism este cu adevărat justificat.

Nu cumva aceste promisiuni pe care – tehnologia informai i< I le face sunt prea bune ca să mai fie şi adevărate? Care suni dezavantajele aduse de aceste promisiuni? Nu este legitim a id întreba care sunt potenţialele efecte ale inovaţiilor tehnologii’ informaţiei? Ce impact vor avea şi în ce măsură avantajele v»< depăşi dezavantajele?

Pentru a căpăta profunzimi noi asupra acestor aspecl* articolul se va focaliza asupra unei arii specifice a războiului, \ anume cea a răspunsului la avertizările timpurii şi starea 4 pregătire militară şi politică împotriva pericolelor ce apar. Articol se va concentra asupra întrebării dacă, şi în ce măsură, ap li caii tehnologiilor moderne ale informaţiei va avea efecte pozitive y sau negative pentru starea de pregătire a comandanţilor militari liderilor politici în contextul pericolelor prezente şi viitoare. 1 ’’

Pentru început, vom prezenta pe scurt esenţa stării

de prcgă|l| politico-militare şi a avertizărilor. Va fi discutat apoi impaoil»)] tehnologiilor informaţiei şi al războiului informaţional asupra câtorva factori cheie prezenţi în aşa-numitul ciclu de intelligence, cum ar fi detectarea potenţialelor pericole, colectarea semnalelor şi modelelor de ameninţare, interpretarea şi diseminarea etc.

După aceasta, va fi pe scurt discutat potenţialul impact al noilor tehnologii ale informaţiei asupra reacţiilor de conştientizare, aşeptare şi evitare din partea liderilor, (vezi şi figura 1). Finalul articolului va conţine câteva concluzii şi recomandări ulterioare pentru studiu.

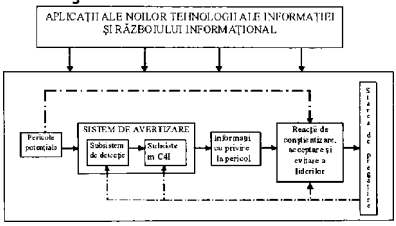

APLICAŢII ALE NOILOR TEHNOLOGII ALE INFORMAŢIEI ŞI RĂZBOIULUI INFORMAŢIONAL
Pericole potenţiale
SISTEM DE AVERTIZARE
Subsistem de detecţie
Subsistem în C4I
informaţii cu privire la pericol
Reacţie de conştientizare, acceptare şi evitare a liderilor
Situaţia de pregătire

Figura 1. Modelul conceptual al analizei prezentate

Starea de pregătire poate fi caracterizată ca fiind un concept familiar, dar în acelaşi tirûp normativ, complex şi interpretabil. Pentru a înţelege implicaţiile dezvoltării continue a tehnologiei informaţiei, este necesar să se înceapă cu o definiţie a stării de pregătire. Definiţia ce urmează combină elementele aflate în descrierile din dicţionare, doctrine militare, studii de război şi proceduri.

Măsura în care o entitate (*prezentată în acest articol ca un grup mic de persoane politice sau militare aflate în poziţii cheie*) *este pregătită la nivel mental, conceptual, fizic, organizaţional şi politic pentru a răspunde pe cât de optim este posibil* (*avându-sc în vedere capabilităţile*) *la diverse pericole din primele faze ale unui conflict*.

Starea de pregătire poate fi privită din perspectiva a trei dimensiuni intercorelate:

1. Prima dimensiune include starea şi oportunitatea anticipării şi vigilenţei mentale (*a factorilor de decizie cheie*), *çuprivire la materializarea pericolelor anticipate, precum sila efectele imediate şi implicaţiile pe termen*

scurt şi lung.

Această dimensiune se referă la gradul în care autorităţile politice şi militare cheie anticipează la nivel conceptual şi mental pericolele. Mai clar, ea cuprinde măsura în care autorităţile politice responsabile au anticipat *mental* o stare de vigilenţă cu privire la:

(a) probabilitatea unei acţiuni ofensive împotriva lor;

(b) tipul acţiunii;

(c) locaţiile unde pericolul (ofensiva adversarului) a acţional;

(d) sincronizarea acţiunilor;

(e) tăria şi punctele slabe ale pericolului (de exemplu, trupele inamice în comparaţie cu punctele forte şi slăbiciunile apărării);

(f) obiectivele ofensivei şi locul acestora în strategia inamicului;

(g) impactul şi consecinţele imediate.

2. A două dimensiune esenţială este formată din starea şi oportunitatea vigilenţei unui factor de decizie, precum şi gradul de pregătire necesar pentru a utiliza componentele conceptuali, fizice şi mentale ale „măsurilor obişnuite" şi „măsurilor de Urgenţă" ccpot fi aplicate imediat când apare un pericol, cu scopul de a minimiza riscurile imediate şi pe termen lung, precum şi Costurile impactului.

3. A treia dimensiune, care poate fi crucială pentru factorii politici de decizie (*în special în timpul operaţiunilor altele decât războiul*), *priveşte gradul în care autorităţile naţionale au acumulat nuficient suport politic, deoarece acesta este necesar unui răspuns optim în faţa pericolului şi consecinţelor sale*.

Această dimensiune se referă la nivelul de anticipare al factorilor de decizie în ceea ce priveşte contramăsurile de protecţie ţi încercările de „educare a publicului" pentru a asigura consensul politic care ar putea li necesar:

(a) pentru a face faţă (de exemplu a minimiza sau preveni) Impactului şi/sau implicaţiilor unui pericol;

(b) pentru a realiza consensul şi sprijinul public şi

politic l itre ar putea fi necesar pentru a asigura fezabilitatea şi eficienţa Unor conlramăsuri rapide, precum şi sprijin pentru implicaţiile Rcestor contramăsuri. Acest lucru include sprijinul, sau cel puţin Urccptarea, din partea grupurilor care nu sunt direct implicate în aspectele operaţionale militare (presa, publicul, alte departamente, polenţialii aliaţi) pentru posibilele opţiuni de management al crizei.

„Avertizările" pot fi privite ca: *O combinaţie de indicatori, litodele, precum şi mesaje scrise care pot fi observate, auzite, citite mi reconstituite de unul sau mai mulţi receptori, şi prin care aceste lUtc asigură predicţii mai mult sau mai puţin incerte şi detaliate despre una sau mai multe dimensiuni ale unui potenţial pericol şi pin care acestea creează un interval de timp suficient pentru a ţHVgăti contramăsuri de protecţie*.

Ga şi starea de pregătire, avertizările prezintă mai multe dimensiuni. Cele prezentate în cele ce urmează pot fi identificate hi ce ie mai multe cicluri de intelligence şi procese de avertizare:

(1) conţinutul;
(2) perioada de timp de avertizare;
(3) accesibilitatea;
(4) siguranţa;
(5) calitatea;
(6) cantitatea.

Studii despre comunicaţii publice şi organizaţionale au indicat că aceste dimensiuni, şi în special combinaţia valorilor specifice ale acestor dimensiuni, pot afecta în mod semnificativ gradul de conştientizare al liderilor, precum şi deschiderea pentru acceptare şi reacţie la semnalele de avertizare.

După definirea stării de pregătire şi avertizări, este acum timpul să se discute despre potenţialul impact pe care aplicarea noilor tehnologii ale informaţiei îl are asupra:

(1) procesului de detectare a potenţialelor pericole;
(2) colectării, diseminării şi interpretării potenţialelor

semnale de avertizare;

(3) conştientizării, interpretării, reacţiilor de acceptare sau respingere a liderilor politici şi militari;

(4) stării de pregătire pentru confruntarea cu pericolele actuale şi viitoare.

Pentru agenţii de intelligence ca Agenţia naţională de securitate (NSA – National Security Agency) şi CIA – Central Intelligence Agency, impactul noilor tehnologii ale informaţiei asupra semnalelor de avertizare şi indicatorilor de ameninţare esto în creştere. Sistemele de avertizare timpurie, posibilităţile do interceptare şi ascultare, precum şi posibilităţi tehnologice do colectare vizuală devin tot mai răspândite şi sofisticate.

Experienţe, ca războiul din Golf, testele nucleare ald Pakistanului în timpul crizei cu India din mai 1998, campanii aeriană din Kosovo şi unele mişcări surpriză ale lui Milosevici y ale armatei sale au subliniat necesitatea de a nu supraestima puterci oferită de tehnologia informaţiei. Multe obiecte statice şi în speeiu cele mobile sunt încă dificil de urmărit cu precizie, în speuiil când trebuie identificate de la înălţime, în scurt timp şi în condiţii] meteo proaste. Machetele se pot utiliza încă cu succes pentru a induce în eroare.

Ultimul deceniu (şi în special ultimii ani) sugerează ca, în comparaţie cu posibilităţile de a colecta avertizările, cea mai mare inovaţie în domeniul „stării de pregătire şi atacurilor prin surprindere” pare a fi în ceea ce priveşte diseminarea de intelligence, aspectele legate de sistemele C4I şi ciclurile de luare în deciziilor. În principiu, potenţialii atacatori şi apărători pot profita tn multe feluri de acestea. Nu ar fi însă înţelept să se neglijeze sau minimalizeze influenţele negative ce pot apare.

De exemplu, nevoia în creştere pentru a avea date în timp real poate creşte gradul de conştientizare al comandantului asupra situaţiei, dar în acelaşi timp creşte şansa ca motivaţia analiştilor fi experţilor de intelligence pentru verificări, analize şi interpretare 41 datelor să scadă.

Mai mult ca oricând, analiştii vor trebui să se confrunte cu (lilcma dacă sau nu ar trebui să disemineze date şi să consilieze mperiorii mai rapid, dacă vor să aibă influenţă asupra factorilor di decizie şi să devină o sursa de încredere a comandantului (dar în riscul de a-şi pierde credibilitatea în cazul unei evaluări greşite).

Experienţele trecute şi recente arată că introducerea noilor U hnologii ale informaţiei tinde să aibă un mare impact asupra i» lor mai multe dimensiuni ale semnalelor de avertizare, impact |n multe privinţe încă imposibil de controlat. În continuare este Hnincată o privire mai atentă asupra impactului probabil asupra diverselor dimensiuni ale avertizării.

Dimensiunea 1: Conţinutul

Avertizările cuprind elemente de informaţie cu privire la unul pu tipai multe aspecte ale conţinutului unui pericol iminent:

1, estimare a probabilităţii ca pericolul (atacul) să se ttwlqrializeze (*dacî*);

2. determinarea identităţii precise a atacatorului (*eine*);

3. determinarea tipului acţiunilor şi tehnologiilor implicate (*cum*);

4. identificarea locaţiei care va fi în pericol (atacată) (*unde*);

5. predicţia momentului de timp la care pericolul se poate materializa (*când*);

6. evaluarea motivelor şi obiectivelor ce stau la baza pericolului (*de ce*).

La prima vedere pare evident că introducerea tehnologiilor moderne ale informaţiei va face ca îmbunătăţirea calităţii avertizării în raport cu fiecare din aceste aspecte să se facă mai uşor. Apărătorii vor dispune de semnale, modele şi evaluări ale avertizărilor şi ameninţărilor mai detaliate, sigure şi mai bine controlabile decât oricând înainte.

În acelaşi timp, însă, apar multe dezavantaje şi capcane. ( ) capcană relativ nouă, care este acum mai

relevantă ca oricând, este *sindromul WYSIWYG* (what y ou see is what y ou get). Liderii şi analiştii care au la dispoziţie date în timp real şi adesea vizualizate şi care pot oferi informaţii despre una din dimensiunile arătate mai sus, vor avea adesea dificultăţi în a rămâne prudenţ i în ceea ce priveşte posibilitatea de a se înşela singuri şi/sau de a fi înşelaţi de adversari. Impactul informaţiilor vizuale asupra minţi i umane poate conduce la percepţii greşite şi eşecuri. De exemplu, există întotdeauna şansa ca atacatorul să-şi schimbe planurile în ultimul moment în timp ce apărătorul încă gândeşte şi acţionează pe baza ultimelor imagini pe care le are.

Chiar mai mult, situaţia actuală a pericolelor iminente poate să se schimbe, semnificativ datorită dinamicii situaţiei şi momentului de timp între trimiterea şi primirea semnalelor. Deşi liderii pot fi conştienţi de aceasta, pot fi în schimb supuşi mai mult ca oricând unor presiuni interioare pentru a lua decizii rapide Faptul că aceşti lideri sunt pe deplin conştienţi că alţii văd acelea şi „imagini în timp real" şi ar putea să se întrebe de ce nu se ia ni ei o decizie (de vină poate să fie acelaşi sindrom) poate deveni <> sursă de presiune.

În plus, doctrinele şi instrucţia pot fi cruciale pentru a face trecerea la cicluri decizionale mai rapide decât ale adversarului, aşa cum impactul presei (de exemplu, efecte de tip CRM şi Internet) poate deveni o sursă majoră de termene limită autoimpuse.

Dezvoltările tehnologice pot creşte probabilitatea ca liderii şi analiştii să cadă în alt tip de capcană cognitivă şi psihologică. Aceasta este reprezentată de faptul că oamenii pot deveni obsedaţi de date vizualizate în timp real, acordând o foarte mare parte din timp pentru aceasta. Preţul ar putea fi că ei aproape trec cu vederea elemente complexe şi cruciale de intelligence (care sunt însă mai puţin accesibile şi controlabile) care ar putea oferi introspecţii interesante despre unul sau mai multe aspecte ale conţinutului pericolului iminent.

Dimensiunea 2: Intervalul de timp

Altă dimensiune crucială a avertizărilor este aşa-numitul *interval de* timpântre momentul avertizării şi momentul care este previzionat pentru materializarea pericolului. Această dimensiune este adeseori denumită şi „interval de avertizare”. La modul ideal (din perspectiva apărătorului), avertizările detaliate şi sigure sunt acelea care se produc la un moment de timp la care este posibilă luarea unor măsuri adecvate de protecţie.

Istoria arată că introducerea diverselor tehnologii în ultimele secole are un imens impact asupra intervalului de avertizare. Probabil cea mai revoluţionară schimbare în război şi managementul crizelor a fost creşterea exponenţială a gradului de mobilitate. Această creştere comprimă timpul şi spaţiul, Sporeşte mobilitatea trupelor, capabilităţile ofensive şi defensive.

Pe măsură ce mobilitatea creşte, intervalul de timp pentru contramăsuri scade semnificativ, de la luni sau săptămâni în secolul XIX, la săptămâni sau chiar zile în epoca căilor ferate, tancurilor şi motoarelor cu combustie, la zile sau ore în era aviaţiei şi la ore sau chiar minute în era nucleară (vezi figura 2).

Tendinţa care s-a manifestat în trecut pare a se manifesta astăzi cu şi mai mare intensitate. Utilizarea ultimelor noutăţi tehnologice de către unul sau mai mulţi adversari poate reduce mărimea intervalului de avertizare spre zero. Cum atacurile informaţionale şi operaţiunile psihologice pot să se desfăşoare în tăcere, va fi din ce în ce mai complicat şi câteodată chiar imposibil să se repereze începutul unui atac informaţional sau să se determine cine, cum, şi de ce îl desfăşoară.

Ar putea deveni chiar greu de determinat cât timp pot fi întârziate evaluarea ameninţărilor, luarea deciziilor şi implementarea contramăsurilor până când întreaga infrastructură C4I a apărătorului să fie serios afectată şi un răspuns adecvat să nu mai fie posibil. Rolul crescând al războiului informaţional ridică rapid bariera clasică dintre război şi pace.

Ca o consecinţă, recentele progrese tehnologice pot

pune la îndoială procesele de evaluare şi nivelul de conştientizare ale apărătorului în ceea ce priveşte probabilitatea, momentul de timp, locul, iniţiatorul şi impactul unui atac, precum şi strategia şi tacticile atacatorului. În fapt, tipuri de arme ce rămân neobservate şi computere „silenţioase" există de câţiva ani încoace şi vor exista cu siguranţă şi în continuare.

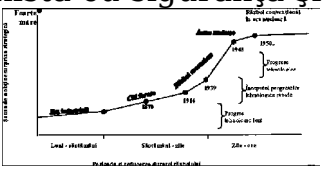


Figura 2. Model conceptual al reducerii duratei războiului datorită inovaţiilor tehnologice şi impactul asupra şanselor de a obţine surpriza strategică

Dimensiunea 3: Accesibilitatea

Una din problemele structurale cele mai mari în legătură cu avertizările care a apărut evidentă în timpul atacurilor surpriză şi confruntărilor cu dezastrele naturale nu este faptul că nu a existat intelligence adecvat la timp, ci faptul că, comandanţii şi autorităţile au fost în mod frecvent informaţi neadecvat de către subordonaţi sau colegi în legătură cu intelligence-ul care a fost colectat şi produs.

Lipsa de accesibilitate poate li cauzată de mai mulţi factori. De exemplu, compartimentarea şi prea multă secretomanie, prea multă specializare şi fragmentare, teama de a pierde credibilitatea în cazul unei alarme false, sindromul „intelligence la comandă", proceduri prea lungi şi complexe etc. Rămâne de văzut dacă beneficiile introducerii noilor tehnologii vor putea depăşi dezavantajele. Într-adevăr, cel puţin teoretic, liderii militari şi politici vor avea mai multe oportunităţi de a beneficia de intelligence şi de a scurtcircuita hăţişurile ierarhice din sistemele C4I.

În acelaşi timp, se poate cu uşurinţă ajunge la tipuri greşite de date, supraîncărcare cu informaţii şi un sentiment fals de control. Mai mult chiar, se poate ajunge

la reacţii greşite în cazul lucrului cu informaţii brute ale căror detalii subtile sunt trecute cu vederea sau prost percepute şi se poate ajunge la ignorarea unor semnale şi indicatori care sunt mai puţin accesibili, dar care pot fi la fel de importanţi în luarea unor decizii corespunzătoare (de exemplu date cu privire la motivaţiile adversarului, strategii şi planuri ascunse).

Dimensiunea 4: Gradul de încredere

Multe din studiile despre răspunsurile la avertizări şi starea de pregătire indică faptul că gradul de încredere al sursei de la Care cineva primeşte semnale şi avertizări are o influenţă semnificativă asupra deciziei dacă trebuie, sau nu, să se acţioneze în urma avertizării. Cu cât este mai mare gradul de încredere al unei surse în ochii beneficiarului, cu atât este mai probabil ca informaţia trimisă să fie acceptată fără o evaluare critică şi se va acţiona pe baza ei. Dacă o sursă nu este considerată de încredere, informaţiile provenite de la ea vor fi mai degrabă evitate sau ignorate. Datorită impactului Internetului şi CRM-ului, ca surse dominante de informaţii în permanentă actualizate, distincţia dintre cele două tipuri de surse de informaţii amintite mai sus devine greu de realizat. Este un paradox faptul că agenţiile de intelligence care frecvent încearcă să afecteze pe alţii prin manipularea informaţiilor diseminate prin Internet şi agenţiile de ştiri pot deveni victime ale aceloraşi mijloace mass-media. Convingerea că eşti capabil de a distinge între informaţii sigure şi informaţii nesigure se poate dovedi o capcană care poate afecta întregul proces de intelligence, cât şi gradul de credibilitate al acestor agenţii.

Dimensiunea 5: Calitatea

Una din cele mai importante dimensiuni a avertizărilor este calitatea, cu alte cuvinte gradul în care o avertizare prezintă certitudine, acurateţe şi predicţii detaliate. Este important de observat că cei mai mulţi factori de decizie trebuie, conştient sau inconştient, să realizeze o evaluare a avertizărilor despre care sunt

preveniţi că nu sunt chiar aşa de încredere şi precise în loc de a face o evaluare post-factum a avertizărilor care s-au dovedit a fi mai puţin precise.

Dimensiunea 6: Cantitatea

Cantitatea avertizărilor primite (adică numărul dé semnale de avertizare primite de agenţiile de intelligence şi factorii de decizie într-un anume interval de timp în raport cu capacităţile lor limitate de a le procesa corespunzător) este una dintre cele mai menţionate dimensiuni ale avertizărilor. La fel ca alte dimensiuni, modul în care cantitatea este folosită depinde de ce semnale, mesaje sau modele sunt denumite avertizări.

Evenimente recente (genocidul din Ruanda din 1994, atacul irakian asupra Kuweit-ului din 1990 sau criza din Kosovo din 1998-1999) arată că este probabilă o creştere spectaculoasă a cantităţii de indicatori asupra potenţialelor ameninţări. Aceleaşi evenimente ilustrează că tehnologiile sofisticate (sateliţi, capabilităţi de intercepţie etc.) împreună cu iluzia creată că a dispune de capacităţi mai bune şi mai rapide de colectare reprezintă o garanţie a succesului, tind să ducă la creşterea „apetitului” organizaţiilor şi factorilor de decizie pentru mai multe date în timp real. Totodată, însă, există şansa ca suprasaturarea cu informaţii a analiştilor, politicienilor şi militarilor să crească.

Facilităţi mai performante vor duce adeseori la creşterea nevoilor comandanţilor şi autorităţilor pentru intelligence detaliat, rapid şi actualizat cu scopul de a creşte gradul de cunoaştere a situaţiei. În acelaşi timp, şi poate că la prima vedere pare paradoxal, este probabil că aceştia vor „trăi” perioade în care se vor simţi „subîncărcaţi” cu informaţie. Se poate distinge aici un model comportamental care este prezent şi în multe alte domenii. Cu cât bunăstarea este mai mare, cu atât aşteptările sunt mai mari, ambiţiile vor fi mai înalte şi frustările în caz de neîmplinire vor fi mai mari.

Studii efectuate asupra atacurilor prin surprindere în ultimele patru decenii au arătat că cele mai multe

avertizări conţin multe semnale distorsionate, precum şi diferite grade de incertitudine şi ambiguitate în ceea ce priveşte toate dimensiunile avertizărilor şi pericolelor iminente.

Unul dintre cei mai importanţi factori implicaţi în eşecuri în privinţa intelligence şi atacurile surpriză este ceea ce se numeşte sindromul „cry wolfCu cât mai multe avertizări şi alerte sunt considerate false (din diverse motive, cum ar fi acela că atacatorul şî-a schimbat intenţiile sau că agenţiile de intelligence au fost iiţsuficient informate despre momentul şi locul apariţiei ppricolului), cu atât este mai probabil ca credibilitatea avertizărilor ulterioare să scadă şi procesul de „desensibilizare” la avertizări să devenină dominant, efectul fiind, bineînţeles, interpretări şi răspunsuri greşite la avertizări viitoare relevante.

De exemplu, în timpul războiului din Coreea, stafful generalului MacArthur, sursa principală de intelligence, a avertizat, pe perioada câtorva luni, Washington-ul despre iminenţa unui atac nord-coreean. Când acel atac a avut loc, secretarul apărării Louis Johnson l-a considerat ca fiind doar o altă violare a frontierei.

Toate aceste avertizări au fost la urma urmei precise deoarece cele două state coreene erau angajate într-o bătălie de artilerie prelungită însoţită de dese treceri ale frontierei. Concluzia care se desprinde este că dacă cineva striga „Lupul! Lupul!” de prea multe ori, s-âr putea ca atunci când într-adevăr apare lupul, să nu-l bage nimeni în seamă.

Este de aşteptat deci ca introducerea noilor tehnologii ale informaţiei nu doar să ducă la creşterea calităţii procesării avertizărilor, ci şi să conducă la diverse forme de informaţii irelevante („zgomot”) şi sindromuri gen „cry wolf \

Inducerea în eroare a fost întotdeauna un element principal al desfăşurării războiului. Se înţelege prin inducere în eroare mascarea intenţiilor reale ale cuiva, a capabilităţilor, manevrelor şi concentrărilor de forţe cu

scopul de a obţine un atac surpriză sau o mişcare defensivă surpriză. Inducerea în eroare este realizată în mai multe moduri:

— răspândirea de zvonuri false;

— mascarea funcţionării legăturilor radio, aranjarea unor reţele radio false, radio-inducere în eroare;

— introducerea unor informaţii false în sistemele de securitate, reţelele de date sau Internet;

— dispunerea unor machete;

— ascunderea obiectelor reale şi a manevrelor pentru a împiedica recunoaşterea şi observarea;

— schimbarea aspectului exterior al obiectelor şi manevrelor;

— producerea de „zgomot” artificial;

— utilizarea viruşilor de computer şi războiului electronic.

Aşa cum războaiele şi bătăliile recente au demonstrat, tehnologiile informaţiei vor juca un rol semnificativ în fiecare din aceste forme de inducere în eroare. Operaţiile informaţionale de inducere în eroare pot determina apărătorii, dar şi potenţialii atacatori, să facă judecăţi şi să ia decizii greşite.

Datorită introducerii noilor tehnologii ale informaţiei în acţiunile de inducere în eroare, oricând ar putea deveni mai uşor pentru un agresor sofisticat să „îndeplinească” aşteptările apărătorului de o manieră bine coordonată, furnizându-i acestuia „ponturi” subtile şi la prima vedere cu un grad de încredere ridicat. Este, de asemenea, mai uşor, cu ajutorul tehnologiei informaţiei, să se pătrundă în ciclurile de luare a deciziilor ale adversarului.

Chiar mai mult, datorită inovaţiilor în domeniul sistemelor de interceptare, poate deveni mai uşor să se verifice dacă, şi eventual în ce măsură, strategiile şi tacticile de inducere în eroare reuşesc.

Studiile din ultimele decenii în domeniul ştiinţelor comunicării, ştiinţelor cunoaşterii şi managementului au subliniat în mod constant că o creştere exponenţială a tehnologiilor de producere a informaţiei a mărit

discrepanţa dintre producerea de informaţie şi capacităţile umane de a utiliza această informaţie. Cu alte cuvinte, producerea şi colectarea mai multor informaţii nu înseamnă strict mai multe informaţii, iar mai multe informaţii nu înseamnă siguranţă, acelaşi lucru cu utilizarea informaţiei.

În timp ce tehnologiile de producere şi diseminare a mai multor informaţii şi într-un mod mai rapid au crescut aproape exponenţial, capacităţile umane de a filtra şi procesa aceste date nu cresc în aceeaşi măsură. Cu alte cuvinte, chiar dacă liderii vor vrea şi vor putea să dispună de mai mult timp pentru procesarea avertizărilor primite, este încă foarte probabil ca multe semnale relevante să fie ignorate. Distanţa între ceea ce analiştii de intelligence şi liderii politico-militari ştiu şi ceea ce aceştia ar putea şti (având în vedere datele pe care le-au avut şi le au la dispoziţie) devine din ce în ce mai mare.

Uneori semnalele vor trece neobservate ca o consecinţă a unor decizii deliberate de a concentra resursele (care sunt puţine) pe interpretarea unui tip de surse şi de a ignora datele din alte surse. Rezultatul este acela că factorii politici vor fi frecvent confruntaţi cu mari discrepanţe între datele puse la dispoziţie, informaţiile pe care le cer, informaţiile de care au cu adevărat nevoie şi datele pe care de fapt le procesează şi utilizează (figura 3).

În această figură, semnificaţia notaţiilor este următoarea:

1. toate informaţiile pe care le are factorul de decizie;

2. informaţiile pe care factorul de decizie vrea să le aibă;

3. informaţiile pe care factorul de decizie are nevoie să le aibă;

4. toate informaţiile despre un anume conflict;

5. semnalele de avertizare despre un conflict anume;

6. informaţiile pe care factorul de decizie le primeşte ca rezultat a strategiilor sale.

Dreptunghiurile nu sunt la scară şi în realitate ele

sunt într-o evoluţie dinamică, depinzând de mediul social al factorului de decizie, de problema în sine etc.

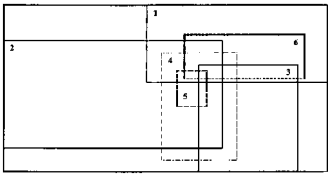


Figura 3. Relaţiile conceptuale dintre diversele forme de informaţii cu care este confhmtat un factor de decizie

Pregătirea, educarea şi exerciţiile

Numeroase ameninţări, precum şi misiuni de tip tactic au nevoie de un înalt nivel de pregătire. Scopul tuturor măsurilor trebuie să fie obţinerea:

Dorinţa individuală şi abilitatea de a accepta responsabilitatea;

Abilitatea de a delega;

Generarea unui înalt grad de sensibilitate în ce priveşte capacităţile potenţiale de operaţii informaţionale ale adversarului;

Dorinţa de a obţine capacităţi adecvate de utilizare tehnică a echipamentului de folosire a tehnologiei informaţionale şi de comunicare;

Educaţia şi antrenarea stabilităţii psihologice a individului pentru a contracara doctrinele şi procedurile adversarului.

Aceasta din urmă merită un interes particular în cazul măsurilor de menţinere a păcii şi/sau de impunere a păcii în cadrul misiunilor Naţiunilor Unite.

Beneficiile unei coaliţii constau în combinarea capacităţilor operaţiilor informaţionale a diferiţilor parteneri, ceea ce furnizează o mai largă varietate de opţiuni şi instrumente în mâna comandanţilor militari. Dar pe de altă parte, noi vulnerabilităţi pot apărea, iar vulnerabilităţile existente se pot multiplica în cadrul coaliţiei.

Chiar dacă fiecare parte s-a adaptat cu succes la provocările operaţiilor informaţionale, fricţiuni există încă

(sau altele noi pot apărea). Aceste fricţiuni care sunt inerente unei coaliţii, provin din surse diferite:

Aspecte umane: Pot exista tensiuni între naţiunile participante, ce-şi au originea în probleme istorice, culturale, religioase sau etnice, de limbaj.

Aspecte tehnice: Interconexiuni ale diferitelor sisteme de tehnologie informaţională şi de comunicare pot duce la posibile piincte slabe.

Aspecte organizaţionale: Structuri diferite de forţe, structuri do C2 sau principii de conducere pot prejudicia operaţiile informaţionale în cadrul unei coaliţii.

Un oponent va încerca să identifice şi să exploateze aceste puncte slabe.

Operaţiile informaţionale defensive

Pentru a contracara aceste vulnerabilităţi şi ameninţări, pentru a veni în întâmpinarea dezvoltărilor viitoare, capacităţile de operaţii informaţionale trebuie să fie dobândite. Acest lucru presupune supravieţuirea pe scară largă a sistemului.

Una dintre cerinţele majore ale unei asigurări informaţionale adecvate este stabilirea unei infrastructuri informaţionale şi de comunicare, de urgenţă, care să fie valabilă 24 de ore din 24 şi 7 zile pe săptămână.

Asigurarea informaţională va deveni o „stare naturală” în cadrul forţelor armate. Pentru a menţine asigurarea informaţională a unei naţiuni sau a unei coaliţii multinaţionale, este necesară o recunoaştere precisă a ameninţărilor operaţiilor informaţionale asimetrice.

Eforturile adversarului de recunoaştere a operaţiilor informaţionale trebuie detectate, analizate şi înţelese. Acest lucru cere o cunoaştere combinată de intelligence şi de operaţii informaţionale. De aceea asigurarea informaţională trebuie să fie considerată ca fiind un interes comun al tuturor ţărilor NATO.

Capacităţi active de operaţii informaţionale ofensive ar trebui dezvoltate în cazul Olandei şi Germaniei. Atunci când te decizi să dezvolţi astfel de capacităţi, spectrul capacităţilor operaţiilor informaţionale dobândite de

ceilalţi parteneri NATO trebuie luat în calcul. În plus, restricţiile legale existente trebuie examinate în scopul de a câştiga o fundamentare juridică solidă pentru folosirea efectivă a operaţiilor informaţionale.

Documentele de politică a operaţiilor informaţionale defensive şi ofensive trebuie publicate pentru a ajuta la clarificarea termenilor, definiţiilor şi responsabilităţilor. O doctrină comună a operaţiilor informaţionale ar trebui publicată şi permanent actualizată. Toate categoriile de forţe ar trebui să-şi implementeze această doctrină.

Folosirea unor astfel de sisteme şi interoperabilitatea ar trebui să fie conduse de necesitatea operaţională, de asigurarea informaţională, supravieţuire, flexibilitate, disponibilitate, performanţă, costuri şi riscuri reziduale.

Deoarece operaţiile informaţionale ar trebui să fie parte integrantă a tuturor operaţiilor militare combinate, este nevoie de planificare şi coordonare printre elementele cartierelor generale integrate, a conducerii şi a altor agenţii.

Un element organizaţional capabil să combine toate aceste activităţi şi să dezvolte orientare şi planificare pentru operaţiile informaţionale poate fi o celulă de operaţii informaţionale (IOC), formată din reprezentanţi din fiecare conducere, componente şi agenţii de sprijin responsabile pentru integrarea capacităţilor şi activităţilor. Figura 2 ilustrează o privire de ansamblu a unei posibile celule de operaţii informaţionale.

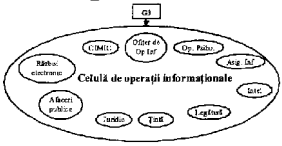


Figura 2: Compoziţia unei celule de operaţii informaţionale

Ministerele de apărare au ocazia să joace un rol important în procesul în creştere a nevoii de asigurare informaţională a altor autorităţi publice şi guvernamentale. Cunoaşterea asupra operaţiilor informaţionale defensive

trebuie împărţită între forţele armate, organizaţiile de apărare civilă, structurile de comandă şi rumurile de industrie critice (energie, transport, comunicare, etc.)

Riscurile fluxurilor informaţionale în cadrul coaliţiilor trebuie bine înţelesă şi de câte ori este posibil, redusă. Componenta de apărare a MEII trebuie privită ca element de sprijin pentru autorităţile civile şi pentru funcţiile economice critice, atât în interesul naţiunii cât şi în sprijinul NATO şi UE.

Acţiuni recomandabile

Grupul de studiu a propus următoarea listă de acţiuni:

Stabilirea unei capacităţi centralizate şi controlate de asigurare informaţională;

Exploatarea cunoaşterii prezente a operaţiilor informaţionale;

Crearea unei structuri de rezervă, de personal, care posedă cunoştinţe şi experienţă în domeniul operaţiilor informaţionale sau care provine din medii etnice, religioase şi culturale (PSYOPS, CIMIC);

Dezvoltarea şi menţinerea unei politici naţionale de operaţii informaţionale (care să se bazeze pe MC 422 a NATO) şi o doctrină integrată de operaţii informaţionale;

Implementarea simultană a politicii comune de operaţii informaţionale de către toate categoriile de forţă;

Cercetarea naţională şi internaţională permanentă în zona de operaţii informaţionale, asigurare informaţională şi protecţic de infrastructură critică;

Definirea la nivel naţional a capacităţilor dorite de operaţii informaţionale ofensive, luând în calcul şi alte capacităţi ale naţiunilor membre NATO;

Definirea şi armonizarea legilor naţionale şi internaţionale;

Stabilirea de celule de operaţii informaţionale la nivele integrate şi combinate;

Definirea unui minim esenţial de infrastructură informaţională naţională, binaţională şi multinaţională;

Implementarea de grupuri de lucru interagenţiale

care sa includă toate sectoarele relevante ale societăţii.

RĂZBOIUL INFORMAŢIONAL PROBLEME şi PERSPECTIVE

vasile păun

Aşa cum am mai afirmat, R.I. este adesea înţeles ca război al epocii informaţionale. Această înţelegere a R.I. se sprijină pe o idee destul de răspândită potrivit căreia societăţile informaţionale succed societăţilor industriale”[41]. Într-adevăr, nurnerizarea, dezvoltarea capacităţilor de stocare a datelor, multiplicarea sateliţilor de comunicaţii creează condiţiile unui mediu foarte diferit de cel cunoscut până în prezent: relaţiile interumane se modifică, apar noi ritmuri.

Cum ar putea ca teoria şi practica războiului să nu fie afectate de aceste schimbări? Ce presupune efectiv un R.I.? Este vorba de o modă pasageră care solicită spiritul imaginativ al analiştilor sau este „principala caracteristică a conflictului secolului al XXI-lea”[42]? Cum abordează statele o astfel de provocare? Ce semnificaţie trebuie atribuită în era Informaţională termenilor utilizaţi în Carta O.N.U.: „forţă”, „atac armat”, „agresiune armată”?

Acestea nu sunt decât doar câteva dintre întrebările care apar natural când se vorbeşte despre R.I. şi care merită o tratare liiai atentă.

EXCURS IN SPAŢIUL CONCEPTELOR

Provocarea nu este de a impune o nouă idee în gândirea militară, ci de a o elimina pe cea veche.

Basil Liddell-Hart

A devenit o obişnuinţă să se vorbească şi să se declare intrarea într-o epocă a informaţiei. „Moda” a venit dinspre Statele Unite unde s-au succedat pe rând mai multe noţiuni cum ar fi cele de „economie informaţională” sau „război informaţional” Din perspectiva soţilor Toffler, anumite state părăsesc societatea de tip industrial pentru a aborda un nou teritoriu, cel al „societăţii celui de-al treilea val”, în care teritoriul, populaţia şi resursele

41 Christian Malis, „Renseignement el information,

42T Atmement", dec. 1997-ian. 1998.

naturale devin mai puţin importante decât capitalul uman, iar faptul de a poseda informaţia potrivită conduce la o modificare sensibilă a activităţii economice, a formelor sociale, a modurilor de conflict.

O expresie des utilizată în mediul militar, în special, este cea a „R.I.”. Sensul exact al termenului nu a fost încă unanim stabilit şi acceptat, mai ales din cauza faptului că acesta descrie un ansamblu de probleme care par să nu aibă nimic în comun. Ambiguitatea termenului creşte pe măsură ce sunt utilizate expresii ca „război în ciberspaţiu”, „război în reţea”, „războiul celui de-al treilea val”, „război post-industrial”[43].

Pentru majoritatea analiştilor militari, R.I. reprezintă o utilizare în scopuri militare a calculatoarelor şi a altor tehnologii împotriva unui stat, ca alternativă la atacurile convenţionale. Acesta include activităţi care nu corespund, în mod normal normelor militare, dar care reflectă creşterea dependenţei activităţilor guvernamentale şi comerciale de diverse sisteme, vitale pentru buna funcţionare a operaţiilor militare moderne

Pentru alţi analişti este vorba de o idee mai largă care juxtapune impactul erei informaţionale eu dezvoltarea diverselor tipuri de conflicte sociale şi politice având ca efect erodarea statu lui-naţiune şi a „monopolului său asupra violenţei organizate”.

O comparaţie cu efectele politice ale primei revoluţii a informaţiei a Europei moderne poate fi utilă. Inventarea modului de distribuţie a cărţilor a favorizat, după anul 1500, transformarea conştiinţei europene. Această transformare a privilegiat, între altele, apariţia statelor-naţiune, asigurând în acelaşi timp conducătorilor posibilităţile de a mobiliza loialităţi naţionale şi de a dezvolta administraţii centralizate. Pe termen lung, cele care nu au avut nimic de câştigat au fost entităţile supranaţionale şi cele subnaţionale (ca instituţia Papalităţii şi autorităţile feudale) care nu au ştiut să profite de noul

43 John Arquilla şi David Ronfeldt, Cyberwarin Coming, RAND, 1992

mediu.

Actuala revoluţie informaţională ar putea avea un efect invers, căci globalizarea şi personalizarea sistemului de Comunicare electronică par să submineze autoritatea statală şi aă uşureze trecerea puterii spre mişcările subnaţionale şi spre cele transnaţionale, mai ales a celor care ating sensibilităţi etnice, religioase sau culturale.

Secolul al XX-lea este caracterizat de îmbinarea dintre ştiinţă şi tehnică (rebotezată cu numele mai nobil de tehnologie). Evident că şi anterior s-au înregistrat progrese remarcabile în cunoaşterea ştiinţifică şi în realizările tehnice |i s-au stabilit legături între teorie şi practică, între domeniul Cunoaşterii „pure” şi cel al „aplicaţiilor”, însă, până în secolul postru, ştiinţa şi tehnologia au evoluat mai mult sau mai puţin N paralel, sprijinindu-se mutual, având însă raporturi cotidiene liai1 degrabă slabe, în a doua parte a secolului al XX-lea (de la M doilea război mondial) electronica a invadat lumea, găsind-o |e afcum pretutindeni: acasă, la locul de muncă, în maşini etc. Calculatorul a abolit, în final, deosebirea dintre ştiinţele „pure” Iau „fundamentale” şi cele „aplicate”, împingând din ce în ce mai departe barierele care, până atunci, izolaseră prelucrarea informaţiei. Ştiinţa este de acum omniprezentă în viaţa materială, iar inovaţiile se succed într-un ritm accelerat. Universităţile nu mai au monopolul cunoaşterii. Ele trebuie să se asocieze cu întreprinderile pentru cercetare şi pentru educaţie. Cercetarea, altădată luxul ţărilor bogate, a devenit un factor de producţie. Munca umană îşi schimbă deja natura. Cuplul, de acum de neseparat, al ştiinţei şi tehnologiei transformă condiţiile prosperităţii şi ale puterii.

Adevărata mutaţie, caracteristică celei de-a doua jumătăţi a secolului al XX-lea, este cea a tehnologiilor informaţionale. Energia şi informaţia, de exemplu, întreţin legături profunde. A obţine o informaţie e ca şi cum ai câştiga energie de calitate superioară, în orice domeniu, a dispune de informaţie înseamnă a merge mai sigur şi mai

direct spre scop şi* în consecinţă, a economisi energie.

În ciuda schimbărilor deja înregistrate, fără îndoială, nu facem decât să întrevedem consecinţele acestei revoluţii informaţionale. Relaţiile internaţionale sunt deja profund afectate de impactul tehnologiilor informaţionale. În prezent, statele controlează pieţele financiare mai puţin decât supraveghează pieţele financiare statele. Astăzi „efectul CNN'\ mâine, fără îndoială, „efectul Internet" este cel ce va invada spaţiul politic.

Este pusă în discuţie problema guvernării societăţilor, pentru că statele sunt prinse în cleşte între influenţele externe, din ce în ce mai constrângătoare, şi creşterea marjelor interne de autonomie (întreprinderi, asociaţii, colectivităţi locale sau regionale etc).

În domeniul militar, armele devin mai precise, mai eficiente şi se diversifică, dar cursa dintre spadă şi scul continuă, ştiinţa putând să servească *a priori* şi unuia şi celuilalt. De aceea, fiu este deloc surprinzător faptul că aceste schimbări influenţează şi operaţiile militare.

RĂZBOIUL INFORMAŢIONAL. ABORDARE TEORETICĂ

Deşi R.I. a fost intuit şi conceptualizat încă din 1976 de către Thomas P. Rona[44], conştientizarea posibilităţii existenţei unui altfel de război, al unui război invizibil, mult mai subtil decât războiul clasic, nu s-a realizat decât foarte recent, tonul dându-l mediile militare.

Una dintre primele pietre de construcţie ale conceptului de R.I. a constituit-o cartea lui A. Toffler, „Al treilea val", apărută în 1980[45]„ În aceasta se poate citi că „pentru a ataca o naţiune se poate obstrucţiona fluxul informaţiilor – tăierea legăturii dintre sediul societăţii multinaţionale şi filialele sale din străinătate, ridicarea de bariere informaţionale în jurul ei etc. Vocabularul internaţional s-a îmbogăţit cu o nouă expresie: „suveranitatea informaţiei"

44[47 Thomas Rona (1922-1997) a creat termenul de „război informaţional" şi a impulsionat cercetările în domeniu.

45 Publicată şi în limba română în 1983, la Editura Politică.

Această reflecţie asupra epocii informaţionale a fost continuată de o altă carte a aceluiaşi autor, intitulată „Război şi anti-război[46]„, care a permis relansarea dezbaterii în Statele Unite asupra conceptului de R.I. Departamentul american al Apărării, care a urmărit aceste reflecţii şi pe care, în mare măsură, le-a şi provocat, a trecut prin mai multe etape, de la conceptul de *Manoeuver Warfare*, aplicabil unui război convenţional, la *Strategic Information Warfare*. Acesta este un concept global care acoperă, în acelaşi timp, noţiunea de *Convenţional Warf are*, care vizează în principal infrastructurile economice ale statului oponent, noţiunea de *Command* & *Control Warfare*, care priveşte în mod clasic distrugerea sau neutralizarea forţelor militare adverse şi noţiunea *Information Warf are*.

Expresia „R.I.” acoperă o serie întreagă de semnificaţii. Lipsa unei definiţii clare a R.I este vizibilă în toată literatura de specialitate. Până în prezent s-a încercat definirea originilor acestui tip de război, însă nimeni nu i-a stabilit încă principiile. Aproape fiecare persoană care scrie despre R.I se confruntă cu această dificultate. S-au formulat, bineînţeles, mai multe definiţii care seamănă între ele. Dar faptul că aproape oricine scrie despre R.I, se simte obligat să-l definească, subliniază această lipsă a unei definiţii universal acceptate.

Teoria şi practica R.I. se bucură, în ultimul timp, de o atenţie crescândă din partea politicienilor, strategilor, oamenilor de ştiinţă şi mijloacelor de informare în masă din diverse ţări, îndeosebi din spaţiul nord-atlantic şi cel european, fenomen uşor de constatat urmărind frecvenţa discursurilor publice, conferinţelor, simpozioanelor, cărţilor, studiilor şi articolelor care abordează această problemă.

Caracteristica de subiect „fierbinte” este de asemenea pusă în evidenţă de diversitatea şi exotismul unor concepte („infrastructură informaţională critică”, „operaţii informaţionale”), specializări universitare

46 Publicată şi de Editura Antet, în 1995.

(strategie cibernetică), instituţii (Colegiul de Management al Resurselor Informaţionale), preocupări („hacker”, „cracker”), toate asociate domeniului R.I.

Deşi nu există o definiţie universal acceptată, se poate vorbi despre RI. ca fiind o formă nouă de război, dacă sunt avute în vedere instrumentele pe care le utilizează pentru a-şi atinge scopurile (graţie în special exploziei tehnologiei informaţionale). Este însă important de notat că tehnologia informaţiei nu permite doar desfăşurarea războiului modern, ci adaugă o nouă dimensiune conflictelor. Infrastructura informaţională, prin conţinutul său şi tehnologiile care o compun, este considerată acum obiect al unui război informaţional, dar şi subiect de aceeaşi complexitate strategică cu dimensiunile tradiţionale (aeriană, terestră, marină şi spaţială).

Reţelele informaţionale compun un nou câmp de luptă, iar informaţia însăşi devine o ţintă. Fiecare a devenit, separat, dar şi în combinaţie cu celelalte, atât armă cât şi ţintă.

În acelaşi timp, se poate vorbi despre R.I. ca fiind o formă veche de război, dacă se face referire la conceptele pe care le are la bază (filosoful chinez Sun Tzu vorbea acum 25 de secole despre „viclenie”, despre arta de a înşela adversarul, despre necesitatea de a împiedica adversarul să evalueze corect o anumită situaţie. Într-un mod asemănător se exprima şi Machiavelli, în secolul al XV-lea, când descria în „Prinţul” sau în „Arta războiului” calităţile omului de stat, ale Prinţului, care, înainte de toate, este un conducător militar ce trebuie să aibă o natură egoistă, calculată, şireată etc.).

După cum am menţionat deja, R.I. nu constituie o practică nouă, din punct de vedere al conceptelor după care se ghidează. Aspecte care ar putea fi considerate ca făcând parte dintr-un RJ. pot fi identificate şi în timpul celui de-al doilea război mondial (acţiunile de dezinformare, de intimidare etc). Însă, elementul de noutate pe care-l aduce astăzi îl reprezintă includerea

mijloacelor tehnice sofisticate existente într-o strategie globală, realizată în funcţie de scopul urmărit.

Această strategie urmăreşte obţinerea unui avantaj, a unei superiorităţi informaţionale faţă de adversari sau chiar faţă de aliaţi.

Iată câteva argumente care marchează diferenţele majore dintre rolul istoric al informaţiei şi teoriile actuale privind R.I:

Superioritatea informaţională era o problemă de noroc şi nu de sistem. Astăzi, R.I. depinde de o exploatare superioară şi sistematică a informaţiei şi de diseminarea la timp a acesteia.

Informaţia a putut influenţa anumite *planuri de război*, dtlf nu şi *execuţia* lor. R.I. cere o avertizare timpurie şi decizii rapide într-un câmp de luptă schimbător.

Războaiele erau câştigate sau pierdute cu sau fără bjtyorul informaţiei. Astăzi, informaţia este primordială, iar Uit R.I cere un flux sigur al ei.

Canalele de comunicare erau în trecut expuse intertaptării. În zilele noastre, tehnologia digitală este extrem de vulnerabilă la interzicerea accesului sau la atacurile care au ca scop manipularea datelor. Atacurile software pot să nu distrugă arme sau forţe, dar pot, cu siguranţă, să le interzică sau să le imobilizeze.

Sintetizând, verbele care se potrivesc cel mai bine pentru a rezuma conceptul de R.I. sunt: a capta, a transmite, a trata rapid o informaţie, a împiedica (adversarul/aliatul să facă acelaşi lucru), a denatura, a dezinforma.

Natura deosebit de complexă a R.I. este evidenţiată de trăsăturile sale:

dificultatea precizării adversarilor absenţa unor frontiere de natură geografică şi/sau temporală multitudinea de ţinte lipsa unor metode rapide de remediere a consecinţelor pe care le generează utilizarea unei tehnologii relativ simple, ieftine şi larg răspândite costurile relativ scăzute ale derulării unui R.I. În raport cu rezultatele ce se pot obţine posibilităţile sporite de

manipulare potenţialul efectului de bumerang ştergerea deosebirilor dintre nivelurile de comandă

Aceste trăsături ale R.I. redimensionează noţiunea de conflict (şi competiţie) adăugându-i noi atribute: *permanenţa*, *transVersaâitatea şi dualitatea*.

Permanenţa presupune aplicarea unei strategii globale care integrează procesele de colectare, protecţie, transport, management şi împiedicare a accesului la informaţie nu numai în perioadele de criză sau conflict.

Transversalitatea semnifică influenţarea societăţii în ansamblul ei şi are la bază conceptele de,,sistem de sisteme" şi „multidisciplinaritate".

Dualitatea se referă la dispariţia deosebirilor dintre sfera militară şi cea civilă. Statele şi forţele armate tind să nu mai aibă monopolul absolut asupra mijloacelor violente şi îndeosebi asupra „violenţei informaţionale"

La nivel naţional, centrul strategic de greutate se mută treptat înspre domeniile bancar, financiar, energetic şi al sistemelor de distribuţie. Infrastructura civilă ajunge cel mai important obiectiv, iar apărarea ei cu forţe convenţionale devine problematică.

R.I. este însoţit de noi mijloace de acţiune/influenţare care eludează puterea convenţională şi graniţele statelor. Multe dintre aceste mijloace acţionează direct la nivelul comenzii şi al controlului, al voinţei, al informaţiei, precum şi asupra elementelor esenţiale ale infrastructurii statale.

R.I. vizează structuri ale domeniului politic, economic, social sau militar, nu doar pentru a le distruge sau paraliza ci, mai ales pentru a le influenţa procesele decizionale. Astfel, se face trecerea de la stadiul de *violenţă organizată* la stadiul de *influenţare ostilă*.

Războiul informaţional se manifestă sub două aspecte: *oâbnsiv* şi *defensiv*.

Războiul informaţional ofensiv include campanii imagologice, acţiuni psihologice în mediul decizional, sustragerea sau vicierea datelor, introducerea de informaţii eronate sau false, interzicerea accesului inamicului la datele proprii, distrugerea fizică a

elementelor care fac parte din uistemele de comunicaţii şi informatică, acţiuni pe Internet etc.

Războiul informaţional defensiv include criptarea, autentificarea şi certificarea datelor şi a informaţiilor, controlul accesului, detectarea şi eliminarea software-ului malign, protejarea informativă şi contrainformativă, contrapropaganda, contrainducerea în eroare.

I În funcţie de strategiile de atac-apărare construite şi de fermele informaţionale utilizate, parte din teoreticienii Accidentali fac referire la următoarele şapte forme de R.I.[47]

Războiul de comandă şi control (forma exclusiv militară a R.I. — are menirea să anihileze comanda şi sistemele de comandă-control ale unui adversar prin integrarea operaţiilor psihologice, a securităţii operaţiilor, a inducerii în eroare, a războiului electronic şi a distrugerii fizice.

Războiul bazat pe informaţii (intelligence) – constă în proiectarea, protecţia şi anihilarea sistemelor care conţin suficiente cunoştinţe pentru a domina un spaţiu de conflict.

Războiul electronic – utilizează tehnologie electronică şi tehnici criptografice pentru dominaţia spaţiului electromagnetic.

Războiul psihologic – utilizează informaţia pentru a modifica atitudinile şi opţiunile aliaţilor, părţilor neutre şi adversarilor.

Războiul hacker-ilor – constă în atacuri cu software „malign”, asupra sistemelor informatice.

Războiul în sfera informaţiilor economice urmăreşte blocarea sau canalizarea informaţiilor şi crearea unei imagini deformate în scopul obţinerii supremaţiei economice.

Războiul în spaţiul realităţii virtuale – foloseşte Internetul drept cutie de rezonanţă şi armă de propagandă

---

473 0 Martin Libicki, "WHAT Is Information Warfare?", National J)Ufense University Press, 1995, http://www.ndu.edu/inss/actpubs/ ti<003/a003.html

la nivel mondial.

Acest mod „tranşat” de a prezenta R.I. este contrazis de Daniel Kuehl[48], care consideră mult mai pertinentă îmbinarea tuturor acestor forme pentru a se obţine o viziune de ansamblu asupra fenomenului R.I.

În funcţie de scopul urmărit, R.I. poate fi purtat[49]:

pentru informaţie – presupunând managementul unei cantităţi importante de informaţii;

prin intermediul informaţiei vizând transmiterea mesajului dorit sau neutralizarea mesajului adversarului;

Împotriva informaţiei – constând în protejarea informaţiilor de posibile manipulări

Aşa cum am afirmat anterior, particularitatea conceptului de R.I, e dată de realizarea unei strategii integratoare care utilizează mijloace tehnice de ultimă oră.

Integrarea pe care R.I. urmăreşte să o realizeze apare pe trei niveluri primare. La un prim nivel, R.I. necesită integrarea ofensivei şi a defensivei. Dacă se doreşte, de exemplu, dezvoltarea metodelor ofensive de R.I., trebuie avută în vedere posibilitatea ca inamicul să poată dezvolta şi el, la rândul său, acelaşi tip de metode.

Cu alte cuvinte, trebuie evaluate consecinţele ce ar putea să apară şi metodele de apărare necesare în cazul în care inamicul recurge la aceste metode ofensive. Orice acţiune ofensivă de R.I. trebuie analizată în lumina impactului potenţial pe care îl poate avea asupra măsurilor defensive proprii, în timp ce orice acţiune defensivă de R.I, trebuie avută în vedere în lumina impactului asupra potenţialului ofensiv.

La al doilea nivel de integrare se află cele şapte forme de război deja menţionate. Fiecare dintre acestea are propriile sale bariere, norme, scheme de clasificare şi mecanisme de observaţie. Dar fiecare trebuie integrată, adică planificată, şi realizată într-o manieră care să completeze şi să îmbunătăţească performanţele celorlalte,

48 School of Information Warfare & Strategy. N.D.U.

49 Jean-Luc Moliner, „La guerre de l'information vue pur im opérationnel français", L'Anmement, nr. 60, dec.!997/ian. 1998

pentru a atinge obiectivele specifice acelui R.I.

Al treilea nivel de integrare are loc de-a lungul trecerii de la o stare la alta, adică de la pace la criză, apoi la război şi înapoi la pace. R.I. are un rol de jucat în fiecare din aceste faze şi acesta trebuie conceput în mod coerent.

R.I. se deosebeşte de atacurile individuale prin faptul că este guvernat de *strategie*, care se concentrează asupra unui *obiectiv*. Strategia constă într-un plan cuprinzător care îmbină armele şi tacticile pentru a-şi atinge scopul. Armele şi tacticilc fot fi orice combinaţie de tehnici, militare sau nu. Obiectivul poate fi militar, politic, economic sau o combinaţie a acestora.

Astfel, o campanie R.I. poate fi dusă în paralel cu alte operaţii de luptă, poate fi dusă dincolo de zonă de luptă şi poate depăşi graniţele în timp de pace, de criză sau de luptă. Termenul de „informaţie” în R.I. sugerează faptul că obiectivul unei âstfel de campanii implică crearea unor efecte în sfera informaţională a adversarului, capabile să-i împiedice sau să-i inspire anumite acţiuni, fapt ce produce un avantaj pentru atacator.

Cunoscând natura războiului informaţional, se constată că adevărata ţintă a tmei campanii R.I. nu sunt sistemele specifice care sunt atacate în momentül respectiv, ci mai degrabă *procesul decizional al* adversarului. Astfel, atacul informaţional trebuie să se bazele nu doar pe caracteristicile acelor sisteme, ci şi pe efecte mai mari.

Acest lucru poate fi ilustrat de un exemplu simplu, atacul menit să bruieze un senzor. Ca operaţie individuală de război electronic, atacul se bazează pe caracteristicile tehnice şi operaţionale ale senzorului. Ca element al campaniei R.I., planificarea şi dirijarea atacului trebuie să se bazeze pe felul în care senzorul contribuie la descrierea situaţiei adversarului şi pe informaţia pe care senzorul o asigură operaţiilor şi forţelor atacatorului. La un nivel mai înalt, acest lucru trebuie să fie luat în considerare în planificarea atacului, iar implementarea este efectul asupra deciziilor adversarului, blocând, degradând sau

falsificând informaţia senzorului. Acelaşi lucru este valabil pentru atacurile asupra sistemelor de comunicare, reţelelor, legăturilor sau centrelor de procesare.

Conceptul general al R.I. poate fi considerat ca având trei părţi: un grup de *elemente de R.I.* (tehnici şi capacităţi), *o sinergie globală s&xe* le aplică şi le orchestrează şi o *ţintă*. *Dom* elementele sunt aceleaşi în cazul R.I. şi al conceptelor tradiţionale de atac informaţional. O definiţie a R.I. trebuie, deci, să descrie obiectivul principal, să identifice şi să enunţe elementele aplicabile ale R.I.,. să arate cum aceste elemente se pot combina în cadrul strategiei de atac al ţintei/

Întrucât obiectivele reprezintă sursa pentru crearea unei strategii a R.I, vom începe cu modelul unei ţinte. Vom trece în revistă, apoi, câteva dintre elementele utilizate în R.I, pentru ca în final, să prezentăm, prin intermediul unui tabel, organizarea elementelor şi relaţiile dintre ele.

ŢINTE ŞI ELEMENTE ALE UNUI ATAC INFORMAŢIONAL

După cum remarca Thomas P. Rona, în sfera militară, sistemele informaţionale cuprind sistemele de comandă şi control, sistemele de *intelligence*, sistemele platformelor de cercetare-lovire şi reţelele de comunicaţii, care constituie infrastructura informaţională a sistemelor menţionate mai sus.

Sfera civilă posedă şi ea echivalentul acestor sisteme critice pentru securitatea naţională (centrele de decizie de la nivel politic, economic, religios, social, de exemplu; infrastructura naţională: sistemele de alimentare cu apă potabilă, cu energie, cu gaz; sistemele bancare, sistemele de telecomunicaţie etc). Practic, aceste sisteme informaţionale (militare şi civile) se sprijină reciproc şi, frecvent, utilizează aceeaşi infrastructură informaţională.

Importanţa acestor infrastructuri informaţionale este evidentă în cazul R.I. Aşa cum se remarcă în studiile de specialitate se pot distinge trei niveluri de ţinte ale unui atac informaţional:

Nivelul sistemelor informaţionale. Neglijând

obiectivul principal, atacurile R.I. se îndreaptă, deseori, asupra sistemului informaţional, care nu întotdeauna reprezintă un sistem electronic. În multe cazuri, acest sistem este ţinta iniţială a atacului, efectele fiind de natură tehnică (supraîncărcarea sursei de recepţie, coruperea datelor, stricarea computerelor, distrugeri fizice etc.). Acest punct este des întâlnit în literatura de specialitate, discuţiile despre RI concentrându-se asupra ţintelor şi metodelor de atac tehnic. Ceea ce nu se are în vedere este obţinerea efectelor operaţionale.

Nivelul gestionării informaţiei. Gestionarea informaţiei se referă la transferul informaţiei, răspândirea, stocarea ei. Efectele sunt funcţionale: o întârziere a informaţiei sau o schimbare la nivelul capacităţilor de transfer al informaţiei.

Nivelul procesului de decizie. Efectele operaţionale ale atacului R.I. de la acest nivel pot fi indirecte: nu se doreşte doar producerea confuziei, ci şi formarea, influenţarea deciziilor, opiniilor adversarului.

Trebuie observat faptul că efectele de la un anumit nivel generează ele însele efecte la nivel superior. De exemplu, un atac menit să bruieze sistemul de informare blochează sau corupe elementele celui care le primeşte (efecte tehnice), iar acest lucru reduce informaţia (efecte funcţionale). Efectul operaţional ar putea fi întârzierea deciziei.

Scopul final al unei campanii R.I, îl reprezintă nivelul procesului decizional. Aşa cum ne sugerează şi Thomas P. Rona[50].

Principala sarcină a nucleului este de a transforma, urmând o logică prestabilită sau propria sa logică, stimulii pe care-i primeşte, în rezultate (comenzi sau mesaje de acţiune către alte nuclee sau către actori externi). Trebuie, de asemenea, observat faptul că nucleul are posibilitatea de a selecta şi de a stabili praguri pentru Stimuli şi de a verifica rezultatul acţiunilor dictate.

---

50 în, »Information Warfare. An Age-Old Concept with New Insights". publicat în Defense Intelligence Journal, 5-1, 1996

Datorită naturii transformatorului logic (fiecare are propria sa experienţă, intuiţie, cultură şi mod de a răspunde la stres) care face foarte dificilă evaluarea modului în care sunt îndeplinite deciziile şi datorită multiplelor căi de atac asupra transformatorului logic, problema mijloacelor de protecţie şi a eficacităţii lor este deseori prost înţeleasă sau chiar ignorată.

Trebuie remarcat faptul că ţările industrializate sunt din ce în ce mai dependente de sistemele informaţionale. În contextul R.I., acest lucru creează noi vulnerabilităţi care se adaugă listei vulnerabilităţilor „clasice” şi care repun în discuţie conceptul de „securitate naţională”

Elementele necesare R.I. sunt:

tehnicile şi capacităţile de atac şi de apărare strângerea de informaţii pentru a localiza informaţia – poziţii, forţe, vulnerabilităţi, apărări strângerea de informaţii pentru avertismente strângerea de informaţii pentru a evalua pagubele

Capacităţile de atac şi de apărare sunt funcţiile fundamentale ale R.I. Acestea pot lua forma unor viruşi în calculatoare, operaţii psihologice etc.

Ca orice alt război, R.I. are nevoie de surse externe. Una dintre acestea o constituie strângerea de informaţii.

R.I. trebuie să fie sprijinit şi de o funcţie de evaluare a pagubelor şi de informaţii de apărare. Pentru aceasta este nevoie de măsuri pentru a putea detecta şi localiza atacurile prin propriul sistem de informare.

Alte elemente-cheie pentru R.I. sunt *expertiza* şi *înţelegerea*. Expertiza tehnică e necesară, dar nu şi suficientă. O înţelegere a ţintei este necesară pentru dezvoltarea unei strategii a R.I.

Orchestrarea numeroaselor elemente ale R.I. este una dintre caracteristicile sale fundamentale. Atacurile combinate sunt aplicate în funcţie de specificul ţintei.

Pentru a şti cum pot fi combinate şi orchestrate diversele clemente ale R.I. trebuie să revenim la modelul ţintei. După divizarea ţintei pe niveluri, fiecare nivel poate fi divizat la rândul său. Urmează o înşiruire a atacurilor

posibile împotriva fiecărui element caracteristic fiecărui nivel. Cunoscând acţiunile şi caracteristicile ţintei putem identifica capacităţile necesare pentru a conduce fiecare atac împotriva fiecărui

Tabelul 1 – Capacităţi specifice R.I.

			Elementele ţinta		
	Logice				
	Iutii	ligence	Informaţie		
	Fizic	Operaţional	Date	Control	
	I x)catie Parametri Funcţii Arhitectur Reţea	Utilizatori Flux de date	Video Text Voce Imaei ne Digital	Stabilirea legaturilor mesajelor Canal comun de avertlizare	

În tabelul 1, legăturile dintre elementele logice şi cele fizice nu sunt arătate, iar relaţiile dintre atacuri/acţiuni de suport şi clementele ţintei sunt prezentate mai puţin sub formă de concepte. Tabelul nu

prezintă nivelurile secundare. Fiecare element poate li divizat la rândul său. Tabelul nu arată acţiunile de apărare şi relaţiile lor cu acţiunile de atac.

În tabel, termenul „intelligence” se referă la informaţia care descrie elementele ţintei. De reţinut că există două tipuri de intelligence: fizic şi operaţional. Intelligence-ul fizic asigură parametrii ţintei şi informaţia structurală sau arhitecturală a reţelelor urmărite. Intelligence-ul operaţional identifică utilizatorii.

Categoria „informaţie” este divizată în „date” (informaţia pe care adversarul o interpretează) şi „controlul informaţiei”

Atacurile asupra controlului informaţiei pot fi o ameninţare Serioasă la adresa reţelelor de comunicare. Categoria „date” este divizată în tipuri, căci acestea definesc capacităţile tehnice necesare pentru atac.

Acţiunile de atac includ măsuri ofensive şi defensive, după cum arată tabelul. Măsurile de atac nu se limitează la blocarea şi coruperea informaţiilor. Cineva poate introduce informaţii l'alse în sistemul de informare al adversarului. Cineva poate utiliza sau nu informaţia obţinută de la adversar, cum indică denumirea „schimb de informaţii” Funcţia „utilizarea informaţiei” se referă la exploatarea informaţiei colectate.

Tabelul este un ghid general şi nu o descriere strictă. Nu loate sistemele de R.I. sau atacurile de R.I. conţin elementele din tabel. Acesta oferă un cadru de lucru pentru căutarea şi Interpretarea capacităţilor şi pentru evaluarea unui R.I.

INFRASTRUCTURILE CRITICE ÎN RĂZBOIUL INFORMAŢIONAL

Când se vorbeşte de orientarea spre ţintă în contextul R.I., ftc fac, de obicei, analogii directe cu războiul cinetic, specific erei industriale: atacuri asupra infrastructurii critice, atacuri asupra sistemelor de comandă şi control etc. Acum sunt avute în vedere şi atacurile asupra computerelor şi sistemelor informaţionale.

La nivelul strategic al analizei, sectoarele infrastructurii critice reprezintă „organele vitale” ale societăţii. În era informaţională, problema care se pune este aceea dacă aceste aspecte ar trebui sau nu să intre în responsabilitatea armatei.

Acestea nu numai că sunt esenţiale bunăstării economice ale oricărei societăţi evoluate, ci şi din ce în ce mai importante pentru viabilitatea forţelor armate ale ţării respective. Sectoarele civil şi militar se suprapun din ce în ce mai mult. Sectoarele infrastructurii critice includ:

sistemele şi reţelele de comunicaţii terestre şi spaţiale sistemele şi reţelele de transport sistemele şi reţelele de distribuţie a energiei sistemele bancar şi financiar sistemele de distribuţie, rafinare şi purificare a apei serviciile guvernamentale esenţiale serviciile de urgenţă (poliţie, pompieri, salvare)

În societăţile evoluate aceste servicii sunt o responsabilitate împărţită de către sectoarele public şi privat. Dar indiferent de cine le gestionează, aceste sectoare ale infrastructurii au în comun un element esenţial: faptul că sunt informatizate într-o măsură din ce în ce mai mare. Progresele în materie de informatică au fost folosite pentru îmbunătăţirea şi eficientizarea serviciilor infrastructurii şi pentru reducerea costurilor operaţionale, însă, pe măsură ce se favorizează eficienţa infrastructurilor critice, se măreşte şi vulnerabilitatea lor.

Referitor la protecţia infrastructurii critice, trebuie luate în considerare patru aspecte ale ameninţării: riscul sinergie (1), ameninţarea asimetrică (2), ameninţarea asincronă (3) şi criza de încredere (4).

1) Statele-naţiune sunt, în principiu, „sisteme de sisteme” elaborate şi complexe. Cu cât naţiunea este mai avansată din punct de vedere economic, cu atât relaţiile infrastructurii sunt mai complexe. Distrugerea sau afectarea gravă a sectorului infrastructurii critice are imediat efecte adverse asupra celorlalte sectoare, şi nu doar la nivel naţional, întrucât sistemele şi sub-sistemele infrastructurii sunt interdependente într-o măsură din ce

în ce mai mare, ele nu pot fi segregate sau izolate într-un efort de limitare a pagubelor.

2) Preocuparea pentru *ameninţările asimetrice* la nivel strategic şi tactic este deosebit de relevantă pentru aspectul protecţiei infrastructurii. O putere mai mică (statală sau nonstatală) poate produce mari pagube unei naţiuni mai robuste, dată fiind dependenţa sporită a acesteia din urmă de infrastructurile critice. Altfel spus, o societate mai puţin dezvoltată este mai puţin dependentă de aceste sisteme atât li zic, cât şi psihologic.

3) O *ameninţare asincronă* poate fi şi ea o problemă pentru societăţile dependente de o infrastructură sofisticată. Atacul fizic asupra unor centre critice pentru societate are efecte vizibile. Dar pot exista şi atacuri punctiforme asupra sistemelor infrastructurii critice, repetate şi extinse pe parcursul unei perioade mai lungi de timp, fără un model exact şi fără un autor imediat identificabil, care pot pune în pericol siguranţa naţională.

4) O problemă îngrijorătoare pe care o ridică o campanie susţinută de atacuri asimetrice la adresa infrastructurii este *criza de încredere publică* ce poate rezulta. Se poate crea iluzia că instituţiile publice şi cele private sunt incapabile de a asigura bunăstarea indivizilor.

Aceste lucruri nu sunt menite să descrie un viitor »pocaliptic. Vor doar să sublinieze gravitatea provocării. Problema pe care o reprezintă protecţia infrastructurii critice este aceea că în societăţile dezvoltate din punct de vedere economic sectoarele public şi privat sunt doar semi-Acestea au scopuri diferite, motivaţii diferite, responsabilităţi diferite şi „produse” diferite. Provocările pe care le ridică cooperarea dintre aceste sectoare se bazează pe trei aspecte: transmiterea informaţiilor (1), aspecte legale (2) şi provocările tehnice (3).

1) Dificultăţile *transmiterii* informaţiilorâşi găsesc originea la nivelul percepţiilor şi încrederii. De cele mai multe ori, sectoarele public şi cel privat nu au încredere deplină unul în celălalt. În mod cert, companiile din cadrul aceluiaşi sector comercial al infrastructurii nu sunt

caracterizate de o încredere reciprocă, în ciuda acordurilor de parteneriat. Există date confidenţiale privind anumite proceduri şi vulnerabilităţi. Pe de altă parte, guvernul, şi în special sectorul de apărare şi securitate naţională, este interesat de informaţiile clasificatc, iar legile şi regulamentele limitează transmiterea şi diseminarea acestora.

Odată ce transmiterea informaţiilor este considerata necesară, ce tipuri de informaţii trebuie să circule între sectorul public şi cel privat, pe de-o parte, şi în cadrul sectoarelor infrastructurii, pe de altă parte? Datele şi analizele privind ameninţările trebuie transmise. Dar ce se întâmplă cu datele şi analizele privind vulnerabilităţile, care se desprind din ce Ic dintâi? Acesta este un aspect foarte delicat.

2) *Aspectele legale* sunt şi ele o problemă. În cadrul sectorului privat există preocupări pentru situaţii precum antitrustul. Există apoi o serie de aspecte legale internaţionale care depăşesc aria de interes a unui stat-naţiune.

3) Există, de asemenea, o serie de aspecte tehnice carc complică procesul colaborării dintre sectoarele public şi privai în protecţia infrastructurii. Acest lucru se aplică mai ales în domeniul tehnologiei informaţionale, iar procesele rezultante de „e-business” şi „e-commerce” schimbă natura întregului sector privat. Pentru acesta din urmă, viteza afacerilor esk principalul motor. Afacerile se dezvoltă şi se adaptează a/i mai rapid decât o va face vreodată guvernul. Această dezvoltare rapidă este posibilă numai în absenţa intervenţiei guvernamentale. Inovaţia tehnologică provine aproape în exclusivitate din sectorul privat. Iată de ce problema colaborării public-privat în protecţia infrastructurii critice se complică.

Aşa cum am afirmat de la început, societăţile avansate se îndreaptă către o sferă nouă, indiferent că aceasta se numeşte sferă informaţională sau ciberspaţiu. În acest demers, omenirea va aduce cu ea vechile ei nevoi şi impulsuri: nevoia de a comunica, de a conversa, de a

comercializa. Ea va aduce cu ea şi impulsul către violenţă, conflict şi război. Iar în procesul acestei migrări, se vor dezvolta şi necesităţi, impulsuri şi obiceiuri noi. Printre acestea se află şi nevoia de protecţie a infrastructurilor critice (fizică şi informaţională).

PROBLEMATICA EVALUĂRII AMENINŢĂRILOR

Imaginaţia este mai importanta decât cunoaşterea
Albert Enstein

De multe ori discuţiile privitoare la ameninţările de tip R.I. se poartă în jurul războiului informatic, în mod special pe marginea vulnerabilităţii calculatoarelor şi a reţelelor. Dacă acceptăm modelul teoretic al lui M. Libicki în care R.I. Înseamnă integrarea a şapte forme de război, focalizarea pe calculatoare este incompletă şi de neînţeles. O ameninţare de lip R.I. ridică, într-adevăr, întrebarea dacă mediul nostru informaţional poate fi manipulat de alţii pentru a câştiga superioritate informaţională, inclusiv utilizând calculatoarele, dar fără a se limita doar la acestea.

Ameninţările R.I. sunt prezente la toate nivelurile (nivelul sistemelor informaţionale, al gestionării informaţiei şi al procesului de decizie) şi, în acelaşi timp, sunt multidimensionale, având o dimensiune politică, economică, culturală, juridică şi nu doar una pur militară, cum greşit se crede.[51]

Aşa cum este ilustrat şi în figura 2, ameninţarea poate fi clasificată în mai multe tipuri, flecare putându-se,,activa" în momentul în care întâlneşte unul dintre elementele unui sistem. Pentru a avea succes este necesar ca cel care lansează atacul informaţional să cunoască foarte bine arhitectura sistemului, modul în care se iau deciziile şi transformatorul logic utilizat (nucleul care ia

51 O prezentare interesantă a ameninţărilor R.I. a fost făcută dc David Alberts în Defensive Information Warfaret N.D.U., 1996. D. Alberts clasifică ameninţările în trei categorii: ameninţări de zi cu zi, ameninţări potenţial strategice şi ameninţări strategice, în funcţie dc aria pe care o acoperă şi de gravitatea consecinţelor lor.

decizii), lucru nu foarte uşor de realizat.

Măsurile de protecţie împotriva ameninţărilor R.I. trebuie să aibă la bază evaluarea ameninţărilor şi avertizarea timpurie.

Evaluarea ameninţărilor trebuie, inevitabil, să ia în considerare vulnerabilităţile. O evaluare completă a riscurilor trebuie să suprapună ameninţările potenţiale şi cele identificate cu vulnerabilităţile sistemelor informatice, pentru a determina nivelul de risc şi a putea planifica răspunsuri.

O ameninţare este o combinaţie de capacităţi şi motive. Puterea unui adversar a fost măsurată până acum în termeni de capacităţi militare şi diverse alte elemente care puteau fi convertite în capacităţi militare, cum ar fi: puterea economică, populaţia şi teritoriul. Indexul compus al capacităţilor este un exemplu clasic în această abordare, agregând elemente cuantificabile din domeniile militar, industrial şi demografic pentru a construi un indicator al puterii naţionale.

Un factor ce trebuie luat în considerare este acela că sistemele de evaluare ale ameninţărilor la adresa securităţii naţionale şi militare au fost în mod tradiţional dezvoltate pentru a evalua capacităţile unor organizaţii.similare din „tabăra adversă”. Din acest punct de vedere, ambele părţi erau organizaţii cu structură ierarhică, funcţionând pe baza unor structuri şi modele uşor de înţeles, în epoca R.I, organizaţiile de tip reţea, prin natura organizării lor, constituie ameninţări la fel de importante ca şi cele de tip ierarhie.

Elemente ale unui sistem	Ameninţări generice						
	Distrugere	Scoatere din funcţiune	Interferenţă	înşelătorie	Saturare	Intruziune	târzie

Obs ervabile		?	?	?			
Surs ele mesajului	?			?			
Com unicaţii	?		?		*		
Man agementu l reţelelor de rnmnni ratif»		*					
Şef		?		*	?		
Echi pă/Experţi		?		*	?		
Mod ele de rleni7ie				?	?		
Proc esori		?					
Bază de date	?			?			

Figura 2 – Ameninţări generice versus elemente importante ale unui sistem

Motivaţiile sau intenţiile acestora sunt mult mai dificil de evaluat decât capacităţile atât pentru analistul de *intelligence*, cât şi pentru factorul de decizie.

Evaluarea ameninţărilor specifice R.I., provenite din mediul substatal, produce cu greutate rezultate clare. Este dificil să acorzi valori clare diferiţilor indicatori utilizaţi şi ar fi, poate, mai utilă folosirea unor metode care să permită cuantificarea prin intermediul unui interval de valori.

războiul informaţional şi legislaţia internâţionalX

Dezbaterile asupra problematicii războiului informaţional au scos deseori în evidenţă problemele tehnologiei modeme, fără a lua însă în discuţie mediul

legal internaţional în care se manifestă epoca informaţională.

Examinarea relaţiei dintre războiul informaţional şi legislaţia internaţională presupune, inevitabil, explorarea câtorva probleme caracteristice: ce reprezintă,,războiul" în epoca informaţională şi ce tipuri de activităţi pot fi numite „război informaţional"? Ce este un act de „război informaţional"? Ce devin „forţa", „atacul armat" sau „agresiunea armată" într-o eră a informaţiei? În ce mod sunt sau pot fi afectate noţiuni ca „suveranitatea naţională", „inviolabilitatea frontierelor"?

Războiul informaţional ridică câteva provocări importante legislaţiei internaţionale actuale.

În primul rând, legile internaţionale definesc starea de război şi starea de pace. Pentru a face această distincţie, nivelul şi natura pagubelor este un criteriu. Pagubele produse de atacurile informaţionale pot fi diferite de cele create de un război tradiţional. Pentru a lua un exemplu, distrugerile cauzatc de bombe sunt uşor de observat, în vreme ce alterarea sau manipularea sistemelor informatice pot produce pagube intangibile, cum ar ti o perturbare a serviciilor de orice natură şi chiar a societăţii, în final. Acest lucru întăreşte convingerea că războiul informaţional este capabil să şteargă linia incertă, din punct de vedere filosofic, dintre război şi pace.

În al doilea rând, până în prezent, statele au constituit subiectul major al legislaţiei internaţionale. Statele sunt entităţi care posedă o autoritate suverană asupra unui anumit teritoriu, însă posibilitatea semnalelor, de exemplu, de a traversa reţele internaţionale pune în discuţie conceptul de suveranitate teritorială naţională, principiu fundamental al relaţiilor internaţionale de la Tratatul de la Westfalia, din 1648, care stabileşte faptul că fiecare naţiune are o autoritate exclusivă asupra evenimentelor care se petrec în interiorul graniţelor sale.

Noutatea tehnologiilor ar putea explica absenţa oricărei măsuri de prevedere explicită în legislaţia internaţională care să interzică practicile ce ţin de

fenomenul cunoscut sub denumirea de „război informaţional” Absenţa unor astfel de măsuri este importantă, căci, în general, ceea ce legislaţia internaţională nu interzice, este permis. Pe de altă parte, inexistenţa acestora nu este hotărâtoare, deoarece chiar dacă legislaţia internaţională nu se referă direct la anumite arme sau tehnologii, principiile sale generale pot fi aplicate şi în cazul acestora.

Conform tratatelor internaţionale şi a cutumei, teritoriul Statelor neutre este inviolabil de către forţele beligerante, în cazul unui conflict, încălcarea frontierelor naţionale, în legislaţia internaţională actuală, se referă în special la acţiunile fizice realizate. Nu se ştie, însă, dacă un atac realizat printr-o reţea care traversează un teritoriu neutru sau utilizează sateliţi, calculatoare sau reţele aparţinând unor state neutre are aceeaşi valoare juridică ca aceea a unei incursiuni a unor trupe înarmate[52].

Astfel de atacuri sunt dificil de încadrat, în momentul de faţă, de legislaţia internaţională. Războiul, în accepţiunea tradiţională, presupune forţe înarmate şi violenţă. Articolul 2 (4) al Cartei O.N.U. interzice ameninţarea sau utilizarea forţei împotriva integrităţii teritoriale Şi independenţei politice a statelor. Însă un atac informaţional reprezintă o „utilizare a foiţei”? Ce înseamnă „forţă”? Aceasta, din perspectiva articolului 2 (4), este privită ca „forţă armată”. Din acest punct de vedere, ne putem întreba dacă un atac informaţional este o „utilizare a armelor”.

Carta O.N.U. conţine două importante excepţii de la regulă, care permit utilizarea forţei armate. Este vorba, în primul rând, de utilizarea forţei având autorizaţia expresă a Consiliului de Securitate şi, în al doilea rând, de utilizarea forţei ca măsură de autoapărare.

Capitolul al VII-lea al Cartei permite Consiliului de Securitatc să autorizeze utilizarea forţei de către state, în cadrul coaliţiilor formate ad-hoc sau în cadrul

52 U.N. Manual on the Prévention and Control of C.omputer-Rclated Crime. 261-264, 1993

organizaţiilor regionale după ce s-a stabilit că este vorba de o „ameninţare a păcii”, de o „ruptură a păcii” sau de un „act de agresiune”.

Întrebarea care apare natural este aceea dacă un atac informaţional poate fi considerat o „ameninţare a păcii”, o „ruptură a păcii” sau un „act de agresiune”, având în vedere caracterul său diferit de cel al unui atac fizic.

Adunarea Generală a O.N.U. a definit „agresiunea” plecând de la o viziune tradiţională a războiului[53]. Declaraţia defineşlo „agresiunea” pe care Consiliul de Securitate este autorizat să o constate drept „utilizarea forţelor armate de către un stat împotriva suveranităţii, integrităţii teritoriale sau independenţei politice ale unui alt stat sau într-o cu totul altă mani eră incompatibilă cu Carta O.N.U.[54] Categoria armelor informaţiona Io ar putea fi acoperită de fraza: (...)”utilizarea oricărei arme împotriva teritoriului unui alt stat”[55]. Un atac informaţional având ca miză „suveranitatea, integritatea teritorială sau independenţa politică” ar putea fi considerat un „act de agresiune” care să determine Consiliul de Securitate să ia poziţie.

A doua excepţie de la regulă o constituie acceptarea utilizării forţei ca mijloc de autoapărare. Articolul 51 al Cartei recunoaşte dreptul inerent la auto-apărare al statelor în caz de „atacuri armate”. Sunt însă atacurile informaţionale „atacuri armate”?

Dificultatea caracterizării anumitor forme ale războiului informaţional ca elemente de „forţă”, „război” sau „agresiune”, din punct de vedere al dreptului internaţional, nu presupune implicit şi imposibilitatea instituţiilor internaţionale de a răspunde la astfel de fapte. Capitolul VII al Cartei O.N.U., de exemplu, acordă Consiliului de Securitate autoritatea şi responsabilitatea

53 Adunarea Generală, Rezoluţia 3314, Déclaration on Agression, din 14.12.1974.

54 Déclaration on Agression, art.l din 14.12.1974.

550 0 Ait.3 (b) al Rezoluţiei 3314, Déclaration on Agression, din 14,12.1974

de a determina existenţa oricărei „ameninţări a păcii” sau a oricărui act de agresiune”[56] şi de a decide maniera de a răspunde la acestea”[57]. Din această perspectivă, multe dintre atacurile informaţionale ar putea fi considerate „ameninţări ale păcii” şi, în consecinţă, ar putea deveni subiecte ale deciziilor Consiliului de Securitate.

Încercările de revizuire a unor aspecte ale legislaţiei internaţionale, care să surprindă mai temeinic fenomenul războiului informaţional, se fac timid simţite. Federaţia rusă, de exemplu, caută să iniţieze un curent favorabil punerii la punct a unei legislaţii internaţionale în privinţa războiului informaţional[58].

Societatea informaţională, dincolo de beneficiile pe care Ic aduce cu sine, ridică probleme importante. Guvernele se confruntă cu probleme fundamentale cum ar fi cele care privesc modul în care se pot garanta valorile democratice într-o societate informaţională. Frontiera dintre starea de pace şi cea de război este tot mai greu de identificat. Unde începe şi unde se termină pacea? Aceasta n-ar putea fi doar un război insesizabil?

Pentru moment există opinii numeroase şi diferite

---

56 Carta Naţiunilor Unite, art. 39, www.icj-cij.org-cijwww-cdocumentbase-Basetext-cunchart.html

57 Carta Naţiunilor Unite, art. 41- 49, w ww. icj-cij.org-cijwww-cdocumentbase-Basetext-cunchart.html

58 In acest sens, Federaţia Rusă a prezentat la a 53-a Sesiune ii Adunării Generale un proiect de rezoluţie privind „Realizările spaţiului informatizat şi al telecomunicaţiilor, în contextul securităţii internaţionaleProiectul de rezoluţie invita statele membre O.N.U, să îşi exprime un punct de vedere asupra utilizării tehnologiilor informatice în scopuri militare, asupra definiţiei conceptelor „arme informaţionale" şi „război informaţional", asupra oportunităţii elaborării unor norme juridice internaţionale privind utilizare« armelor informaţionale, asupra necesităţii creării unui sistem internaţional de monitorizare a ameninţărilor legate de securitate» informatică şi de sistemele de telecomunicaţii (a 53-a Sesiune n Adunării Generale, 08.09-18.12.1998, punctul 64 pe ordinea de /i „Menţinerea securităţii internaţionale: Prevenirea degradării violente a Statelor").

privind necesitatea surprinderii la nivelul legislaţiei internaţionale a activităţilor informaţionale şi maniera în care acestea pot deveni subiecte ale dreptului internaţional, dat fiind că fiecare dintre acestea este motivată de interesele proprii.

În ciuda acestei stări de fapt, nu se poate trece cu vederea faptul că noţiunea de „război”, aşa cum este ea definită de Carta O.N.U., tinde să devină o noţiune depăşită de evenimentele timpului nostru. Carta nu evoluează în acelaşi ritm cu realităţile de azi şi tinde să ofere toi mai greu o imagine adecvată a lumii actuale.

VULNERABILITĂŢI ALE TEHNOLOGIEI INFORMAŢIEI

MAARTEN VELTMAN[59] RICHARD L. PARKER[60]

Toate sistemele de tehnologia informaţiei şi comunicaţiei (ICT) au vulnerabilităţi. Slăbiciunile acestor sisteme sunt introduse în timpul uneia din fazele de stabilire a specificaţiilor, implementării sau fazei operaţionale. Lăsând deoparte faptul că aceste vulnerabilităţi pot aveaun caracter intenţionat sau neintenţionat, trebuie luat în considerare că aceşti factori fac ca securitatea informaţiei să fie la fel de puternică ca legăturile ei cele mai slabe.

O echipă de profesionişti – o echipă roşie – are ca scop combinarea capacităţillor tehnice necesare cu practica în vederea identificării şi evaluării acestor vulnerabilităţi. Primul pas în desfăşurarea analizelor efectuate de echipa roşie este culegerea de informaţii urmată de analize pe zone (site), rezultând un raport complet şi accesibil. Mijloacele şi tehnicile utilizate de cele mai performante sunt aceleaşi cu cele utilizate de hackeri în prezent pentru sisteme de calcul şi reţele de calculatoare.

Experienţa dovedeşte că dezvoltarea de metode şi menţinerea unei legături de cooperare cu personalul responsabil sunt cruciale pentru formarea unei echipe roşii

59 Laboratorul de fizică şi electronică, Olanda.

60" Agenţia NATO Hagâ, Olanda.

profesioniste.

Toate sistemele de tehnologia informaţiei şi comunicaţiei (ICT) au vulnerabilităţi. Odată ce un calculator sau o componentă reţea este introdusă într-un sistem, vulnerabilităţile acelei componente expun restul sistemului la riscuri. Există în mod normal trei surse care generează puncte slabe în sistemele de securitate – specificare, implementare şi operare.

Punctele slabe specifice specificării şi implementării suni de obicei identificate prin experienţă sau analize de laborator şi se concretizează în petece (*patch-uri*) sau actualizări (*upgrad-ări*). Dar chiar şi cel mai sigur sistem poate să aibă vulnerabilităţi introduse prin practici defectuoase de operare/configurare.

Cele mai moderne sisteme de ICT au posibilităţi de comunicare şi aplicare bazate pe setul de protocoale TCP/IP. La momentul specificării lor, aceste protocoale nu au abordai aspectele de securitate aşa cum le cunoaştem noi astăzi; ele au fost proiectate pentru a fi utilizate într-o comunitate de conectare restrânsă unde toţi membrii aveau încredere unul în celalalt.

Există unele aspecte ale acestor protocoale care sunt în prezenl puţin problematice. Protocolul de transfer al fişierelor (FTP), de: exemplu, nu numai că permite obţinerea unui fişier prin conectare la distanţă, dar de asemenea permite unui utilizator conectat la distanţă să şteargă şi să înlocuiască fişiere de pe server. În mediul specific zilelor noastre, trebuie luate măsuri pentru a asigura ca numai utilizatori de încredere conectaţi la distanţă au aceste capabilităţi, altfel modificarea web-site-ului ar fi un element mu Îl mai cunoscut decât este în realitate.

Implementarea vulnerabilităţilor poate fi neintenţionată sau intenţionată. Vulnerabilităţile neintenţionate sunt destul de cunoscute – inadvertenţe software (*bug-uri*). Uneori, aceste inadvertenţe conduc către breşe de securitate posibile (ex depăşirea de memorie generează blocarea unui program într-o zonă

temporară privilegiată, rezultând o încălcare a drepturilor de acces) sau uneori pot genera comportamente nedorite (ex. blocări ale ecranului). În oricare din cazuri iniţiatorii nu au dorii ca aceste manifestări să aibă loc şi când o astfel de inadvertenţ; este descoperită, apare foarte repede un petic sau o modificare; programului pentru a corecta problema.

Implementarea intenţionată« vulnerabilităţilor este cu totul altă problemă. În unele cazuri acestea pot fi de tipul „uşa din spate” sau „cal troian” lăsate în urmă pentru a permite programatorului să exploateze funcţii ascunse dintr-o anumită componentă de echipament. Un exemplu uzual a acestui tip de cod este omniprezentul „*Easter Eggs* – Ouă de Paşti”. Ouăle de Paşti reprezintă în mod curent un cod nedăunător lăsat în urmă de iniţiatori şi este invocat de un anumit trigger de intrare (filtru de interogare) sau trigger eveniment; funcţionalitatea pe care o reprezintă nu are nimic de-a face cu funcţia declarată a programului.

Având astfel identificată cu grijă locaţia oului în cadrul modulului executabil, modificarea sau înlocuirea codului ar putea fi realizată fără o diferenţă observabilă în operarea programului şi fără modificarea dimensiunii fişierului. Este ingrijorător faptul că cineva ar putea şterge codul Oului Estic şi să-l înlocuiască cu ceva dăunător, cum ar fi un modul de modificare sau redirectare a datelor la salvarea fişierelor.

O parte a problemei stă în practica standard de furnizare a configuraţiilor implicite pentru sisteme ce le fac cât mai uşor de activat şi rulat. În scopul de a spori posibilitatea componentelor sistemului de a opera „potrivit specificaţiilor”, configuraţiile implicite sunt proiectate pentru a fi cât mai „tolerante” posibil – permiţând cea mai largă variaţie a condiţiilor în care componenta va opera. De exemplu, o staţie Sun Spare este configurată în mod uzual pentru a accepta un domeniu larg de servicii reţea (ex. email SMTP şi sistemul de fişiere în reţea (NFS)).

Uneori configuraţiile acceptă funcţii de securitate ce

nu sunt integrate suficient în sistemul de operare existent. De exemplu, nu este de niciun folos dacă elementele de securitate cum ar fi conectarea şi verificarea sunt instalate, dacă ieşirea nu este niciodată verificată sau utilizată de personalul autorizat sau funcţiile automate. Un alt exemplu larg răspândit este utilizarea de parole slabe (sau neexistente) pe timpul procesului de identificare şi autentificare (*login*). Exemple ca acestea fac operatorii să se întrebe de ce elementele „de securitate” au fost instalate pe primul loc.

Chiar atunci când o componentă sistem este configurată iniţia I pentru a reduce numărul de vulnerabilităţi, configuraţia componentei se modifică în timp. Sunt instalate noi pachete software şi sunt făcute actualizări de sistem; utilizatorii şi operatorii modifică parametrii pentru a aduce schimbările corespunzător cerinţelor operaţionale. Mai departe, mulţi din aceşti parametrii nu sunt -independenţi şi astfel schimbările pot introduce efecte colateralc neprevăzute. Toate aceste aspecte combinate fac aproape imposibilă estimarea în ansamblu a posturii de securitate a unui sistem ce cuprinde un mare număr de servere, staţii de lucru şi componente de comunicaţii.

În ultimii ani, specialiştii în securitatea informaţiei (InfoSec) au început să se bazeze tot mai mult pe o tehnică de analiză numită „echipa roşie”. Numele este împrumutat din exerciţiile militare curente unde forţele gazdă au asociat indicativul de „echipa albastră” şi forţele opuse au asociat indicativul de „echipa roşie4' Prin jucarea scenariului împotriva unui „inamic” activ, tactici Ic şi strategiile pot fi revăzute şi rafinate. În lumea ICT, sistemele operaţionale sunt revizuite pentru vulnerabilităţi de securitate de o echipă de specialişti de InfoSec, utilizând mijloace şi tehnici speciale dezvoltate pentru aceasta, şi uneori împrumutate de la adversarii potenţiali – *hackeri*.

Restul acestui articol detaliază natura echipei roşii InfoSec, tipurile de mijloace şi tehnicile implicate, felul

rezultatelor ce pot fi obţinute şi unele observaţii bazate pe experienţa de echipă roşie.

La sfârşitul anului 1993, Dan Farmer şi Wieste Venema au realizat lucrarea intitulată „îmbunătăţirea securităţii site-ului dvs. prin pătrunderea în el”.

Lucrarea a avertizat operatorii să înceapă să analizeze securitatea sistemelor lor prin abordarea acestora din punctul de vedere al hacker-ilor. Această lucrare a anunţat de asemenea realizarea unui produs denumit Sistemul de Administrare a Securităţii pentru Analiza Reţelelor, prescurtat SATAN. SATAN automatizează o serie de verificări de vulnerabilitate realizate în mod curent în sistemele Unix.

El s-a bazat pe munca prealabilă făcută de Farmer pentru COAST şi CERT (COPS – Calculator Oracle şi Sistemul de Parole) şi munca prealabilă a lui Venema, incluzând filtre TCP. Lucrările ° Există dragoni” şi „Pachete găsite pe Internet” scrise de Steve Bellovin au detaliat traficul reţea asociat cu încercările hacker-ilor, cartea lui Bellovin şi Cheswick „Ziduri de foc şi securitatea Internet: interviu cu hacker-ul Willy”, sunt câteva lucrări şi numeroase eforturi contemporane au condus la stadiul curent al practicii în domeniul analizelor vulnerabilităţii de reţea/ sistem, bazate pe sisteme de probă pentru vulnerabilităţi cunoscute sau suspectate „din afară”, utilizând tehnici de exploatare pentru determinarea posturii de securitate a sistemelor ţintă.

Aceste documente şi activităţile pe care ele le reprezintă formează baza analizelor de securitate a sistemelor ICT bazate pe scanarea activă a vulnerabilităţilor exploatabile – echipa roşie. Echipe de specialişti care dispun de mijloace hardware şi software special construite pot oferi în acest mod analize independente a posturii de securitate a sistemului.

În timp, personalul, metodele şi tehnicile pentru realizarea acestui tip de analize de vulnerabilitate au devenit mai specializate, migrând de la sisteme de operare, la roluri dedicate în analizele de vulnerabilitate.

Din nou, împrumutând tehnologia din domeniul militar şi dorindu-se, în parte, adoptarea acestor tehnici de către organizaţiile militare cum ar fi Agenţia Sistemelor Informaţionale ale Apărării (DISA), şi Centrul de Război Informaţional al Forţelor Aeriene (AFWIC) în SUA, acest proces a devenit cunoscut ca „echipa roşie”.

Formarea şi utilizarea unei echipe roşii nu este totuşi o problemă simplă. Găsirea membrilor în echipă cu capabilităţi tehnice corespunzătoare poate fi dificil de realizat. Mijloacele necesare pentru acest tip de activitate pot fi scumpe şi nu întotdeauna îndeplinesc aşteptările. Personalul responsabil pentru asigurarea securităţii sistemelor este posibil să nu aprecieze venirea unei echipe care să prezinte zonele în care sistemul este deficient. Orice element subiectiv poate să influenţeze eforturilor de analiză: conflicte de personalitate, interpretarea greşită a rezultatelor etc.

Formarea unei echipe poate să fie prima provocare reală. Persoanele implicate în acest tip de activitate sunt de obicei celc cu indemânări tehnice performante, cu un larg spectru de cunoştinţe în domeniul tehnicii de calcul, a protocoalelor de comunicaţii. Cei mai mulţi au experienţă în dezvoltarea şi/sau operarea câtorva din aceste componente. O condiţie necesară este „nevoia de a cunoaşte” cum lucrează sistemele, de jos până la nivelul de înţelegere a structurilor de date şi a secvenţelor de interschimb specifice proceselor de IT.

Aceste caracteristici (diversitatea şi puterea personalităţilor ce le însoţesc de obicei) au făcut dificilă asamblarea mai multor grupuri de analişti capabili de a realiza analize de tipul „echipă roşie”. Din fericire, uneltele şi tehnicile sunt disponibile mai structurat, făcând posibilă instruirea personalului mai puţin oriental tehnic în ceea ce se utilizează ca fiind ceva de adevărată artă mai curând decât o practică binedefinită.

Cât timp un grad acceptabil de abilitate tehnică este necesar pentru a aplica complet uneltele şi tehnicile şi pentru interpretarea corespunzătoare a rezultatelor,

înţelegerea îndeaproape a modului de lucru intern a componentelor de IT nu mai este necesară. Specialiştii InfoSec cu o înţelegere detaliată a structurii interne a sistemelor de IT sunt persoane necesare pentru analize şi contramăsuri la vulnerabilităţile noi şi complexe precum şi pentru furnizarea de sfaturi pentru echipele roşii operaţionale. Selecţionarea şi familiarizarea cu „unelte de cumpărăt" devint următoarea provocare majoră.

Pentru cea mai mare parte, aceste unelte colectează împreună vulnerabilităţi şi exploatări cunoscute, automatizează sarcina de verificare a sistemului şi necesită o mai slabă înţelegere a tuturor detaliilor despre toate vulnerabilităţile din partea utilizatorilor.

Unele dintre aceste unelte sunt dezvoltări comerciale (ex. Analiza de Securitate Kane), unele sunt disponibile gratuit (ex. Scotty/Tkined, NTCrack) şi unele sunt câte puţin din ambele (ex. ISS Internet Scanner oferă atât o versiune gratuită limitată cât şi o versiune comercială cu toate capabilităţile).

Tabelul de mai jos prezintă un scurt subset de unelte utilizate pentru a detecta şi corecta (sau exploata) vulnerabilităţi în sistemele de operare şi aplicaţii larg răspândite în componentele de comunicaţii din zilele noastre, staţii de lucru şi servere. Uneltele au fost grupate pentru simplificarea inţelegerii capabilităţilor lor generale. Sublinierile n-ar fi trebuit plasate pentru stabilirea categoriilor lor ci ar trebui să se concentreze pe înţelegerea posibilităţilor şi aplicaţiilor lor.

Analize de vulnerabilitate

Internet Scanner, Kane Security Analist, Trident IP Toolbox/ L3 Expert, Security Profile Inspector (SPI), NAI CyberCop, SATAN

Monitorizare reţea

Sniffer, Etherpeek, TCPDump, Snoop, IPWatcher, T-sight, Scotty/Tkined Detectare intruşi

NetRanger, Stalker, Intruder Alert, Network Flight Recorder Exploatare

Crack4, Offline NT Password Utility, NTCrack, CDC

Back Orifice

Altele notabile

Ted wrappers, Tripwire, COPS, crack, ScarmT, Nmap port scanner

Tabelul 1; Unelte de tip „echipă roşie”

O dată ce echipa a fost constituită şi uneltele selectate, începe adevărata parte dificilă – obţinerea acceptării comune şi domeniul de experienţă. Cât timp activitatea de laborator este necesară, nu există substitut pentru experienţe operaţionale. Învăţarea cum trebuie rulat şi analizat cu întreruperi minimale şi efect maxim nu este un exerciţiu abstractă, reprezintă cunoştinţe obţinute prin experienţă.

Tipurile de vulnerabilităţi care pot fi găsite de către echipele roşii sunt diverse. Ele diferă de la probleme tehnice, organizaţionale, la probleme sociale şi în unele cazuri ele se suprapun.

Începând cu o perspectivă tehnică o structură uzuală de reţea poate fi recunoscută. Cele mai multe reţele care sunt în atenţia echipelor roşii constă din aceeaşi structură reţea şi aceleaşi elemente de reţea. La nivel fizic vor exista cabluri de reţea şi fire care fac posibilă comunicarea între elementele reţelei. Router-ele şi comutatoarele oferă un mijloc de canalizare a traficului dintr-un loc într-altul. Mai mult vor exista sisteme ce oferă servicii pentru staţii de lucru sau clienţi.

Acţionând ca un utilizator de nivel mediu cineva n-ar putea să aibă grijă de toate aceste elemente, mai puţin în situaţia în care ele nu sunt funcţionale. Din perspectiva utilizatorului, serviciile cele mai uzuale ar trebui să fie poşta electronică, accesul la fişiere, interogarea web şi posibilitatea de a participa la noile discuţii (ale organizaţiei).

Luând aceste servicii generalizate ca o bază, cineva poate uita uşor că există o mulţime de protocoale în spate care fac posibile aceste servicii. De exemplu, protocoalele ce facilitează serviciul de poştă electronică este Protocolul de Transfer al Poştei Simple (SMTP), Protocolul Post Office

(POP) şi Protocolul de Acces al Mesajelor Internet (WAP). Lăsând deoparte standardele şi protocoalele afiliate cu aplicaţia de poştă electronică ceea ce trebuie observat este că toate aceste protocoale au propriile lor chichiţe, legate fie de specificaţii, implementare sau operare. O echipă roşie va încerca să puncteze problemele legate de elementele slabe de securitate privind integritatea, autenticitatea, confidenţialitatea şi disponibilitatea.

Abordând vulnerabilităţile din perspectiva tehnică a ceea ce ar putea să exploateze o echipă roşie, poate fi făcută clasificarea următoare.

Colectarea informaţiilor despre structura reţelei ţintă, sistemelor şi utilizatorilor care o exploatează, este un punct de start bun. Aproape toate informaţiile care pot fi obţinute pot fi folositoare fie direct fie indirect într-o situaţie viitoare. Această informaţie, chiar fără sens la prima vedere, poate ajuta la identificarea punctelor slabe. Informaţiile din această categorie sunt clasa şi tipul sistemului de operare şi clasa şi tipul de servicii oferite. Lăsând deoparte serviciile directoare pentru utilizatori publici, care conţin o informaţie bogată, în unele cazuri sunt incluse adresele personale de acasă şi numerele de telefoane.

Exemplu: O modalitate de obţinere a unei vederi de ansamblu privind serviciile oferite de un server este determinarea tipului de servicii care sunt oferite (ascultate) pentru conexiunile la acel server. Într-un mediu bazat pe TCP/IP utilizarea normală a binecunoscutelor servicii este limitată la numerele de port TCP/IP stabilite exact. De exemplu serviciile FTP sunt oferite pe portul 21, e-mail (SMTP) pe portul 25 şi www pe portul 80. Prin trimiterea cererilor de conectare la toate numerele de port şi înregistrarea răspunsurilor obţinute este uşor să spună ce servicii sunt ascultate (acceptate) şi astfel oferite.

Această tehnică populară este cunoscută sub denumirea de *scanarea porturilor*, O dată ce toate informaţiile sunt colectate, poate fi făcută o căutare pentru vulnerabilităţile cunoscute care se potrivesc sistemului de

operare detectat, serviciilor şi versiunii.

O tehnică foarte cunoscută pentru a creşte (a spori) un privilegiu este exploatarea unei legături de încredere între două părţi de încredere. O implementare bine-cunoscută a acestei tehnici este numită *spoofmg* (imitaţie). Cele mai multe protocoale şi servicii au deficienţe privind mecanismele bune de identificare a părţii care expediază pachete. Tehnica *spoofmg* utilizează aceste prescurtări pentru a falsifica sursa unui pachet. Când partea receptoare primeşte acest pachet falsificat el presupune că este în comunicaţie cu gazda de încredere adevărată când de fapt el are de-a face cu atacatorul.

Altă metoda de a exploata o legătură de încredere este forţarea (*hijacking*) unei conexiuni existente între două părţi de încredere. Fără măsuri adecvate, numai stabilirea conexiunii este autentificată. Modalitatea cea mai răspândită pentru autentificare este prin tipărirea unui nume utilizator şi a unei parole. Odată ce sesiunea este stabilită este posibil să se intre în sesiune Iară să mai fie nevoie de re-autentificare. Evident această tehnică este numită forţarea conexiunii (*conection hijacking*).

Exemple concrete ale exploatării legăturii de încredere este modul cum programele utilitare pot conduce la erori. Echipa de Răspuns de Urgenţă pentru Calculatoare (CERT) avertizează despre acest tip de atac în sfaturi CERT 95-01.

„Uşa din spate reprezintă un nume al familiei de programe de tipul Cal Troian care deschid noi vulnerabilităţi de securitate pentru sistemele pe care sunt executate”. O uşă din spate poate fi introdusă fie pe timpul fazei de dezvoltare de către programator, sau într-un stadiu ulterior de către atacator. Prezenţa şi aplicaţiile uşilor din spate pot fi foarte puternice. O echipă roşie poate utiliza uşile din spate documentate/cunoscute sau poate să introducă propriile uşi.

Un exemplu pentru mediile Unix este RootKit. Acesta constă dintr-un set de unelte de modificare sistem (ex. login) echipat cu uşi prin spate. O dată ce un hacker a

obţinut controlul asupra sistemului de operare Unix, el înlocuieşte uneltele sistem adevărate cu cele din RootKit. Uneltele sistem modificate oferă posibilitatea de a obţine accesul în sistem prin utilizarea uşilor din spate instalate.

În mediile Microsoft Windows un exemplu popular este programul hacker „Back Orifice". Esenţa exploatării constă în faptul că programul de tip Cal Troian trebuie să fie instalat şi activat pe sistemul ţintă de câteva ori. Modul uzual de a realiza asta este prin trimiterea unei anexe e-mail pentru utilizatorul ţintii ignorant. Prin ascunderea Calului Troian într-un mic joc, imagine sau felicitare, acesta se va activa când utilizatorul ţintă deschide mesajul. O dată instalat, controlul complet asupra ţintei este garantat, prin conectarea la distanţă utilizând mouse-ul şi tastatura. O demonstraţie a acestui atac face utilizatorii să fie informaţi despre riscurile care sunt introduse prin executarea anexelor e-mail ne verificate.

Termenul de interzicere a serviciului sună maliţios şi într-un anumit fel aşa şi este. Totuşi atacurile controlate de interzicere a serviciului pot fi de folos pentru alte atacuri, de exemplu exploatarea legăturii de încredere explicată mai înainte. Atacurile de interzicere a serviciului pot exista pe multe straturi. Un exemplu dat aici se referă la protocolul care este utilizat în cadrul Internet numit TCP/IP. O parte a protocolului este orientat pe conexiune Protocolul de Control al Transmisiei (TCP). Unul dintre cele mai bine cunoscute exemple de interzicere a serviciului cu TCP este numit inundare sincronă (*SYN-flooding*). În continuare vom intra în unele detalii tehnice.

Stabilirea unei sesiuni TCP constă dintr-un proces numit strângere de mână pe trei căi (*three-way Handshake*). Acest proces este reprezentat în figura 1.

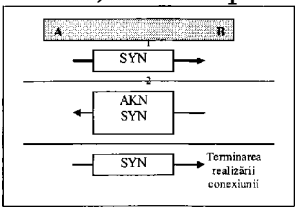


Figura 1: TCP/IP strângere de mână pe trei căi

Ne imaginăm că un client A vrea să stabilească o conexiune cu serverul B. Pentru a începe conexiunea clientul va trimite un pachet ce indică dorinţa lui de a stabili (sincroniza) o conexiune (SYN). Serverul B va confirma că a recepţionat acest pachet prin trimiterea unui pachet de confirmare (luare la cunoştinţă) (SYN+ACK).

În această etapă conexiunea este pe jumătate deschisă. Pentru a încheia strângerea de mână pe trei căi clientul A va emite un semnal că a luat la cunoştinţă despre pachetul recepţionat de la serverul B (ACK). În acest moment clientul A poate să schimbe date cu serverul B.

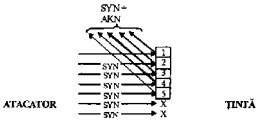


Figura 2. Exemplu de interzicere a serviciului: inundare SYN

Una dintre problemele cu setarea de mai sus este numărul limitat de sesiuni care pot fi în stare de deschis pe jumătate pe serverul B. Acest număr de sesiuni este numit *backlog* (conectări în fundal) şi depinde de tipul sistemului de operare, dar în mod normal va fi în jur de 4-6 sesiuni. Dacă clientul nu ia cunoştinţf de pachetele trimise de server, serverul va trata această sesiune că a depăşit timpul (*time-out*), va reîncerca restabilirea de câtcva ori şi în final va şterge detaliile din *backlog*.

Durata totală a acestui proces fi de 10 minute. Acum să ne imaginam scenariul descris în figura 2.

În combinare cu tehnica de spoofmg explicată mai devreme, atacatorul va forţa un număr de solicitări de stabilire a conexiunii (destul ca să umple *backlog-ul* serverului). Ţinta crede că, comunică cu o gazdă, alta decât atacatorul. Această gazdă nu este capabilă totuşi să răspundă (fie este prea ocupată lie este inexistentă). În acest moment ţinta nu va accepta noi conexiuni (*backlog-ul* lui este plin oricum) şi va aştepta până când fie primeşte

luările la cunoştinţă pentru conexiuni sau ajunge la depăşire de timp.

Această tehnică numită *SYN-tlooding* reprezintă o interzicere a serviciului foarte eficientă. Atacatorul are nevoie să trimită câteva pachete false la fiecare 5 sau 10 minute pentru a realiza scoaterea efectivă din funcţiune a ţintei. Acest tip de atac este puţin utilizat astăzi, dar cu doi ani în urmă el reprezenta o vulnerabilitate exploatată frecvent. Atacul pasiv este un atac fără ca ţinta să-şi dea seama că este supusă unui atac. Un exemplu de atac pasiv este posibilitatea de a citi toate pachetele de pe firele de conexiune, tchnică cunoscută sub denumirea de *sniffing* (strănut) sau *snooping* (sughiţ). Pe timpul operării normale o placă de interfaţă la reţea (NIC) prelucrează numai pachetele destinate plăcii proprii şi le trimite la nivele superioare. Prin punerea plăcii într-un mod special (mod dubios) toate pachetele care ajung la NIC vor fi prelucrate. Utilizarea legitimă a acestei caracteristici ar trebui administrată în reţea şi corectată.

Totuşi, posibila utilizare greşită a acestei caracteristici este mult mai profundă. Programe specializate se găsesc pe Internet şi identifică sesiunile de autentificare necriptate (care pot include parole) sau alte date senzitive. În general tot traficul necriptat este marcat, acesta include e-mail şi sesiuni Web. O echipă roşie poate utiliza această tehnică pentru o diversitate de motive. Uneori informaţia culeasă scoate în evidenţă că ţinta lucrează cu materiale Hcnzitive sau secrete, într-o manieră neadecvată sau într-o reţea ncsecretă. În alte cazuri informaţia poate fi utilizată pentru a lansa noi atacuri asupra sistemelor sau pentru a extrage parole pentru iccesul neautorizat la sistemele ţintă.

Majoritatea atacurilor pot fi plasate în această categorie. Cele mai multe pachete software comerciale de scanare a vulnerabilităţilor cum ar fi *Internet Security Scanner* (IIS) şi *Network Associates CyberCop* identifică găurile în software sau într-un sistem de operare. Din cauza diversităţii lor nu poate li dată o descriere generală.

Un bun exemplu ce explică impactul posibil este dat mai jos.

Serviciile cele mai uzuale cu care oamenii se ocupă în prezent sunt prezentate la nivel aplicaţie. Servicii ca poşta electronică (SMTP), protocolul de transfer al fişierelor (FTP), şi WWW (HTTP) sunt cele mai cunoscute. Una din vulnerabilităţile de implementare a acestor protocoale este numită în mod curent depăşirea de memorie (*buffer overflow*).

Depăşirea de memorie apare când se plasează un obiect de o anumită dimensiune într-o zonă de memorie prea mică rezervată în acest scop. Un exemplu practic este procesul de conectare (*îogin*) utilizând parole. În mod normal o parolă nu va depăşi un număr de 16 caractere. Ce se va întâmpla dacă sunt inserate 300 sau chiar mai multe caractere la dialogul de interogare a parolei? O interpretare grafică este descrisă în figura 3.

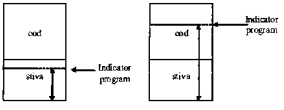


Figura 3: Principiile care stau în spatele depăşirii de memorie (overflow).

Situaţia normală (simplificată) este reprezentată în situaţia I. Poziţia actuală a rulării programului sursă este păstrată de un contor numit contor de program. Valorile de intrare sunt stocate în stivă, care este dinamică. Programul va citi informaţia de intrare, o va pune în stivă (ex. parola) şi o va şterge după ce termină utilizarea ei.

Când nu sunt făcute verificări de limite aceste valori de intrare pot, dacă depăşesc zona de memorie alocată, să suprascrie alte părţi de program, incluzând codul program (vezi situaţia II). Comportamentul normal când au loc depăşirile de memorie se manifestă printr-o interzicere a serviciului. Totuşi dacă datele de intrare sunt puse într-un mod special cineva poate să suprascrie codul program cu noi instrucţiuni program.

Efectul tuturor acestora ar fi că de exemplu procesul de autentificare (în cazul exemplului cu parola) execută cod arbitrar introdus de atacator. Acest cod va rula în contextul de securitate al procesului în chestiune, procesul de autentificare. Dacă contextul de securitate este destul de înalt, poate fi obţinut întregul control al sistemului de operare.

Pentru punerea acestei teorii în practică un atacator are nevoie să cunoască poziţia precisă (deplasamentul) pentru codul care trebuie inserat. Cu toate vulnerabilităţile, o dată ce oamenii găsesc una dintre ele, sunt realizate pentru utilizare publică scripturi şi unelte automate la scurt timp după anunţarea acesteia. Cele mai multe depăşiri de buffer exploatează codul de protecţie inserat din care va răsări o rădăcina de protecţie ce va da controlul total atacatorului.

Când sunt primite sfaturile de securitate de la Echipa de Răspuns de Urgenţă pentru Calculatoare (CERT) şi Recomandări pentru Incidente Calculator (CLAC) pot fi găsite avertizări pentru aceste vulnerabilităţi de depăşire a memoriei. Un exemplu este recomandarea CERT 07 (16 iunie 1999). Având un zid de foc activat, dacă este configurat şi menţinut corect, el poate preveni multe atacuri. Dar ce se întâmplă dacă utilizatorii folosesc staţii de lucru echipate cu modem-uri pentru a realiza propria lor conexiune la Internet sau la alte reţele. Zidul de foc (*firewall*) al corporaţiei va fi de eficienţă redusă. O modalitate pentru echipelc roşii să identifice acestea şi sistemele corespunzătoare este utilizarea echipamentului pentru scanarea domeniului telefonic pentru modem-urile active.

În unele cazuri modem-urile găsite sunt instalate de cătrc administratorii de reţea pentru a facilita managementul de la distanţă. O idee nobilă dar mortală, dacă este utilizată de către altcineva. Pe lângă vulnerabilităţile tehnice, o mulţime de erori rezultă din lipsa unei (bune) politici de securitate şi a măsurilor organizaţionale, care includ proceduri pentru

managementul operaţional, managementul de schimb, politica utilizată pentru acceptare etc.

În practică, echipele roşii găsesc adesea în lucru versiuni ale sistemelor de operare sau ale serviciilor care au vulnerabilităţi cunoscute. Deşi sunt disponibile actualizări, petece sau corectări oferite de vânzător, administratorii aleg să nu instaleze acestc corectări dintr-o varietate de motive. Consecinţele pot să fie dezastruoase.

Exploatarea unei vulnerabilităţi cunoscute într-un sistem identificat ia mai puţin de o secundă pentru a distruge zile sau săptămâni de muncă. Datorită creşterii interconectivităţii, răspândirea informaţiei referitoare la vulnerabilităţi este foarte rapidă. Când cineva din SUA găseşte o vulnerabilitate şi publică detalii despre ea, unelte pentru exploatarea ei vor apărea la scurt timp după acesta şi sistemele de la alt capăt al lumii vor fi atacate în aceeaşi zi. Administratorii nu au altă variantă decât acţionarea fermă şi mulţumirea cu securitatea informaţiilor oferită de vânzătorii lor şi/sau echipele CERT când este posibil.

În alte cazuri securitatea funcţiilor este implementată dar nu este pusă în funcţiune. Administratorii sunt mai mult decât fericiţi dacă au reuşit să instaleze pachetele software cu succes, iar ultimu I lucru în mintea lor este să depună efort pentru activare;

elementelor de securitate. Aceasta se reflectă în istoria şi modul de desfăşurare al proceselor, prin punerea accentului pentru proiectarea reţelei şi a sistemelor mai mult pe funcţionalitatea dorită şi pe uşurinţa utilizării. Cerinţele de securitate sunt (cu noroc) pe locul doi în această proiectare. Aşa cum s-a menţionat înainte, tehnologia anilor 1970 (TCP/IP) pe care Internetul se bazează, nu are măsuri standard pentru oferirea de confidenţialitate, autenticitate şi integritate.

Şi chiar dacă funcţiile de securitate sunt implementate, puterea unui sistem se reflectă în legăturile sale slabe. O situaţie cu care echipele roşii se întâlnesc frecvent este utilizarea de parole slabe sau a nici unei

parole pe durata procesului de identificare şi autentificare, care te face să te întrebi de ce acest element de „securitate” a fost instalat pe primul loc.

Dar chiar parole dificile sunt sparte în timp de ore sau chiar minute. Principiul din spatele celor mai mulţi spărgători de parole, nu este posibilitatea decriptării parolelor, ci compararea parolei criptate cu rezultatul criptat al unui set de caractere de intrare utilizat. Spărgătorii de parole utilizează astfel două abordări.

Atacul dicţionarului. Prin criptarea cuvintelor dintr-un dicţionar şi compararea rezultatului cu parola criptată. Dacă parola aleasă este listată într-un dicţionar este o problemă de minute înainte ca parola să fie găsită. Cineva ar fi surprins să vadă cum mulţi oameni utilizează cuvinte uzuale sau nume ale activităţilor lor. Cum ar fi „bună încercare dar nu merge”. Cei mai mulţi spărgători de parole verifică automat diferite variante ale dicţionarului prin adăugarea de cifre sau prin despărţirea în silabe.

Forţa brută. Toate combinaţiile de caractere posibile sunt criptate şi comparate cu parola criptată şi care vor conduce eventual la parola căutată. Deoarece programul popular de spargere de parole pentru Microsoft Windows NT declară: *„Toate piirolele alfanumerice pot fi găsite într-un interval mai mic de 24 i*|(> *ore pe un Pentium 11*|*450*”.

Pe lângă mijloacele tehnice de obţinere a informaţiilor, modalitatea tradiţională de obţinere a informaţiei poate fi la fel de fructuoasă. Când se face un test de pătrundere în interior, o observare fizică a camerelor unde sunt situate ţintele poate fi o posibilitate. Un fapt de viaţă este că oamenii tind să scrie lucrurilc pe care au nevoie să şi le reamintească.

Altfel spus, nume de login, parole, nume de sistem şi chiar informaţii personale cum ar fi numerele cărţilor de credit şi numerele de securitate socială sunt scrise şi stocate într-un loc accesibil membrilor echipei roşii. Informaţia obţinută poate ajuta de asemenea la ghicirea căii de urmat pentru intrarea în sistem. De multe ori sunt utilizate numele comune sau numele legăturilor lor ca bază

pentru parole. Această tehnică numită *ghicirea de parole*, *reprezintă* noroc chior.

Pe lângă informaţia stocată pentru reutilizare, de asemenea lucrurile aruncate după caz la coşul de gunoi pot fi folositoare. Există chiar un nume asociat acestei tehnici care este *trashing* (recuperare).

Un nivel adesea uitat, dar cu toate astea foarte puternic, este-, nivelul mental. Acest nivel se referă la mijloace psihologice de influenţare a oamenilor. O tehnică angajată de unii hackeri este *ingineria socială*.

Imaginaţi-vă comportamentul utilizatorilor unei reţele a corporaţiei când cineva sună spunându-i că el este administratoru I reţelei: *„Domnule, noi avem o problemă cu utilizatorii bazei noastre de date, unele înregistrări au fost şterse din greşeală. Puteţi să-mi spuneţi parola dvs. aşa încât să pol să repar înregistrările* ' Aţi fi surprins să vedeţi câţi oameni sunt gata să ajute dându-şi parola. Sau ce se întâmplă când oamenii din departamentul de management al sistemului primesc o scrisoare de la vânzătorul echipamentelor lor, care le spune că este nevoie neapărat să instaleze programul de corectare (*patch*) inclus. Când este instalai „patch-ur va introduce o uşă prin spate pentru atacator. Aceasla va lucra garantat dacă departamentul de management al sistemului va primi scrisoarea cu câteva zile înainte de Crăciun.

Destul de impresionant este că multe echipe roşii nu utilizea/a în prezent aceste tehnici, care dacă sunt utilizate într-o maniera corectă pot fi foarte utile vizavi de programatori sau de educarea utilizatorilor.

Prevenirea exploatării vulnerabilităţilor sociale este chiar dificilă. Parte a acesteia trebuie să fie realizată prin politici utilizator acceptabile şi educarea utilizatorilor. Pe de altă parte, pentru menţinerea nivelului de securitate există o mare preocupare pentru ceea ce se spune şi comportamentul asociat al utilizatorilor.

Fiecare efort de analiză este diferit de alt efort şi nu este posibil să fie realizată o „carte de bucate” pentru abordarea unei echipe roşii. Totuşi, este posibil să se ofere

o vedere de ansamblu a modului cum un astfel de grup îşi face treaba. Procesul descris aici este aplicabil sistemelor ce au conexiuni de reţea externe (ex. Internet). Pentru sistemele ce au conectivitate externă, o parte a tuturor analizelor de vulnerabilitate poate fi realizată dintr-o locaţie de la distanţă.

Efortul unei echipe roşii începe de obicei cu o cerere sau sugestie ca un anume sistem să fie subiectul unei analize. Odată ce autorităţile abilitate sunt de acord cu activitatea de analiză, cchipa roşie începe să colecteze orice informaţie disponibilă despre structura sistemului analizat. Înainte de a face asta trebuie îndeplinite posibilele aspecte legale.

Aceasta necesită ca echipa roşie să aibă o clară înţelegere a limitelor reţelei din „cyberspaţiu” care urmează să fie analizate. Aspectele legale ar trebui să fie bine înţelese şi cunoscute dinainte. Ar trebui considerate de asemenea riscurile de accesare neintenţionată a reţelelor din afara limitei intenţionate.

De exemplu, când o evaluare este făcută pentru vulnerabilităţile reţelelor din Olanda, legea infracţiunii prin calculator, Directiva Europeană pentru Intimitate Privată şi legea telecomunicaţiei restricţionează echipele roşii în „libertatea” lor de a opera. Evident proprietarul reţelei analizate ar trebui să-şi Isuine responsabilitatea dată de abordarea profesională şi limite legale ale echipei roşii. După ce toate aceste aspecte au fost Iau mate, echipa roşie poate să înceapă treaba.

Mai întâi, tipologia fizică a reţelei este detaliată – dacă reţeaua utilizează cablu coaxial, cablu cu două fire, sau fibră Ethernet; locaţia, modelul şi tipul de router-e, bridge-uri şi hub-uri. Pe urma este topologia logică a reţelei – locaţia serverelor cheie (ex. DNS, Web); spaţiul de adrese de IP şi orice subreţea ce este implementată. Frecvent, este de mare ajutor realizarea unei diagrame sau desenarea componentelor cheie ale sistemului de analizat.

Atât vederile de ansamblu cât şi de detaliu sunt folositoare, dar invariabil devine necesară producerea unei

singure diagrame ce arată toate componentele semnificative pe o singură pagină, fără să depindă cât de mare sau cât de mică este acea pagină pentru ca toate componentele să fie lizibile. Pe cât posibil* e nevoie ca această informaţie să fie colectată înainte de etapa activă a analizelor de vulnerabilitate. Este o muncă dificilă, dar înţelegerea întregului sistem aflat în analiză este crucială pentru succesul întregului efort.

Având colectată în avans cât mai multă informaţie, echipa roşie trece la faza vizibilă de analiză pe site. Aici este locul unde sunt aduse unelte de analiză de vulnerabilitate, *sniffere*, unelte de mapare (întocmire hărţi), pachete de desenare şi alte unelte de reprezentare documentată a sistemului aşa cum este el implementat. Pe cât este de important să existe suport local şi coordonau: pentru această fază a analizei, pe atât este, de asemenea, important să se evite transformarea vizitei site-lui într-un eveniment special, făcând imposibilă obţinerea unei viziuni imparţiale a operării normale a sistemului.

Deoarece surprizele nu sunt plăcute pentru nimeni, este important să se limiteze cunoaşterea dinainte a vizitei echipei roşii la un număr de câteva persoane. Pentru a evită conflictele, personalul local cunoscător trebuie să fie disponibil pentru a trata orice preocupări sau furnizări greşite din partea responsabililor care nu au fost informaţi cu privire la efortul de analiză.

În general, o echipă roşie va avea sisteme portabile încărca în cu pachetele software necesare pentru realizarea analizelor <K vulnerabilitate – uneltele menţionate mai sus. Echipele roşii ar trebui echipate, de asemenea, cu o mare varietate de componente de reţea pentru a facilita accesul la sistemele aflate în analiză.

Cabluri, hub-uri reţea, testere de cablu, prize triple de alimentare, conectoare, adaptoare, multimetre, role de cablu, unelte de prindere, unelte de lipit, unelte de mână, o imprimantă portabilă şi multe altele vor fi toate utile la un anumit moment dat. În timp, fiecare echipă va colecta setul de unelte de care are nevoie, dar este întotdeauna

mai bine pentru o echipă roşie să fie dotată complet, decât să implice personalul al cărui sistem este analizat.

Membrii echipei vor pierde de obicei câtva timp să verifice informaţia culeasă înainte şi să colecteze orice altă informaţie care lipseşte din datele iniţiale. În particular, este importantă verificarea dacă topologia actuală a unui sistem se potriveşte cu documentaţia. Semnalarea discrepanţelor minore poate schimba semnificativ rezultatele de ansamblu.

De exemplu, o conexiune reţea furnizată pentru posibilitatea configurării de la distanţă când un sistem este prima dată instalat, poate fi uitată şi lăsată acolo până când sistemul este complet pus în funcţiune. Verificarea setului documentat de servicii de informaţii este, de asemenea, important, deoarece fiecare serviciu de informaţii aduce propriul set de vulnerabilităţi pentru serverele şi clienţii implicaţi. O dată ce topologia sistemului şi informaţia a fost verificată, echipa poate identifica elementele cheie (ex. servere primare, clienţi obişnuiţi, elemente reţea cheie) pentru analize de vulnerabilitate detaliate.

După ce vulnerabilităţile au fost identificate, echipa roşie începe procesul de elaborare a unui raport pentru autoritatea care a autorizat analiza. Există trei aspecte cheie a modului în care această fază a procesului decurge. Mai întâi, raportul de trebuie să fie complet şi accesibil.

Raportul este de mică valoare dacă nu explică vulnerabilităţile şi nu sugerează remediile într-o manieră care poate fi înţeleasă şi ipoi pe baza lui acţionat de către personalul responsabil pentru sistemul subiect. Unele dintre uneltele angajate într-un efort de analiză generează documentaţie ca parte a operării lor; combinând ieşirile acestor unelte cu alte informaţii (ex. diagramele de topologie a reţelei) pentru a produce un raport succint şi complet este o altă parte a activităţii echipei roşii.

În al doilea rând, nimănui, dar nimănui, nu-i place să fie apostrofat. Pentru a pune asta în context, este esenţial ca rezultatele unui efort de analiză să fie discutate cu

personalul afectat de acestc rezultate, cu participarea sau contribuţia autorităţii de autorizare, înainte ca rezultatele să fie prezentate în întregime structurii de management/comandă implicate. Aceasta permite personalului afectat să înţeleagă rezultatele şi implicaţiile fără să fie pus în situaţia de apărare şi să crească probabilitatea de recepţie pozitiva a rezultatelor.

În final, echipa roşie trebuie să-şi amintească faptul ca rezultatele analizelor aparţin autorit&ţii autorizate. Rezultatele analizelor de topologie a reţelei, datele de vulnerabilitate colectate: şi raportul însuşi sunt informaţii privilegiate şi nu ar trebui să fie oferite altora fără permisiunea expresă în primul rând a entităţii care a autorizat analiza. De fapt, este uzual pentru echipele roşii să utilizeze calculatoare notebook, cu drivere de disc înlocuibile astfel îricât echipele pot lăsa toate datele reziduale autorităţii de autorizare.

Din nou, deoarece aceasta nu este o descriere completă a tuturor consideraţiilor şi activităţilor ce au loc pe timpul unei analize a echipei roşii, ea oferă unele incursiuni în operaţiile unei astfel de activităţi. Pentru a înţelege echipa roşie mai complet, este probabil cel mai bine să fie realizate pentru câtva timp unele analize de vulnerabilitate de laborator, şi apoi să se treacă la activităţi de teren.

În timp, fiecare echipă găseşte combinaţiile de unelte, tehnici şi personal ce se potrivesc cel mai bine sistemelor pe care ei le analizează. Frecvent, unelte similare multiple vor fi utilizaţi separat sau în combinaţie. De exemplu personalul echipei roşii; Agenţiei NATO C3 (NC3A) utilizează de obicei două tipuri de analiză LAN diferite (ex. sniffers), ţinând cont pe de-o parte de posibilităţile diferite ale celor două produse şi pe de altă parte de preferinţele individuale ale membrilor echipei.

Membri diferiţi din echipă vor aplica tehnici diferite pentru obţinerea aceleiaşi informaţii. Cineva adept al sistemului Unix va selecta probabil utilizarea programului snoopmai curând decât o analiză de LAN externă.

Un grup va prefera scanarea de vulnerabilităţi pentru ISS, pe când altul utilizează CyberCop şi un alt grup va lucra cu ambele unelte. Familiarizarea cu un număr mare de unelte şi câteva implementări ale fiecărui tip de unealtă este mai importantă decât selectarea „celei mai bune unelte”. Şi „trusa de unelte” a echipei se va schimba în timp.

Dezvoltarea unei metode de lucru a echipei este probabil mai importantă decât selecţia uneltelor. Personalul va avea nevoie să petreacă câtva timp să lucreze cu uneltele proprii în laborator pentru a se familiariza ei înşişi cu operarea şi interpretarea corectă a rezultatelor. Ei trebuie, de asemenea, să petreacă ceva timp pentru a lucra unul cu altul, să vadă care e modul de lucru al fiecărui membru al echipei şi care sunt punctele lui slabe şi tari. Acest aspect s-a dovedit a fi crucial, deoarece membrii capabili ai echipei obişnuiau frecvent să aibă o contribuţie de leader în activităţile profesionale anterioare.

Echipele roşii trebuie de asemenea să dezvolte o metodă de lucru cu personalul responsabil de sistemele pe care echipa le va analiza. Aici este foarte important să se menţină legături de cooperare şi nu de adversitate.

Echipele roşii vor fi angajate frecvent ca un pas în procesul de acreditare a sistemelor operaţionale precum şi pentru revizuirea posturii de securitate a sistemelor existente. În ambele cazuri, este important să existe o coordonare apropiată cu operatorii sistemului, o aprobare din partea structurii lor de management/comandă. Este de asemenea important să fie utilizaţi cel puţin doi sau trei analişti în fiecare efort, atât pentru a împărţi munca cât şi pentru a furniza „două pereche de ochi” pentru problemele importante. Când este posibil, este de asemenea de ajutor să fie desemnat un membru special al echipei care să se ocupe de orice problemă apărută între echipa roşie şi personalul operaţional local.

Aspectele cheie menţionate în secţiunea precedentă despre activităţile echipei roşii şi aplicabilitatea lor, au

pierdut din vedere un aspect minor dar nu l-au uitat – costurile formării şi menţinerii unei echipe roşii. Pe scurt aceste costuri sunt substanţiale. Cum s-a menţionat mai înainte este nevoie de unelte şi software specializate, lăsând deoparte disponibilitatea unor profesionişti de încredere cu performanţe şi cu o instruire ridicată.

Suplimentar procesul complet de culegere de informaţii, analiza pe site şi raportarea rezultatelor în timp. Efortul final trebuie făcut pentru optimizarea procesului în derulare, specific metodelor şi tehnicilor echipei roşii pentru a asigura că acele cunoştinţe imediate despre noile dezvoltări şi tehnologii devin disponibile.

O echipă roşie joacă un rol modest până la unul efectiv în tabloul mai mare al domeniilor securităţii şi siguranţei informaţionale. Totuşi, tipurile de vulnerabilităţi care pot fi găsite pe timpul activităţilor echipei roşii sunt de folos în procesul de dezvoltare şi de menţinere a bazelor securităţii informaţiei – politica de securitate. Politica de securitate descrie procedurile organizaţionale şi măsurile tehnice pentru a reduce şi elimina riscurile.

Fără o astfel de politică, un incident întâmplător poate duce la o pierdere financiară considerabilă. O echipă roşie va oferi o parte a soluţiei prin identificarea şi raportarea punctelor slabe într-o infrastructură de tehnologia informaţiei concretizată prin luarea de măsuri adecvate. La final este mai bine să previi şi să stai departe de necaz în loc să aştepţi ca lucrurile să se întâmple.

Operaţiile informationale un mijloc de descurajare strategică

ANCA MONICA POPA

Mediul informaţional actual devine tot mai complex, dezvoltarea tehnologiilor informaţionale revoluţionând modul în care naţiunile, armatele, organizaţiile şi oamenii interacţionează. Fuziunea reţelelor de informaţii, a bazelor de date şi a tehnologiilor aduc informaţia foarte aproape de fiecare. Avantajul informaţional presupune cunoaşterea foarte bună a ceea ce înseamnă informaţie şi abilitatea de a lucra cu o colecţie de informaţii, de a o procesa, utiliza şi

disemina în locul, la momentul şi pentru scopul potrivit.

Exploatarea avantajelor oferite de puterea tehnologiilor informaţionale, alături de o recunoaştere a potenţialului informaţiei, se reflectă în ceea ce este numită operaţie informaţională.

Aplicarea de operaţii informaţionale (O.I.) în cadrul coaliţiilor în timp de pace, înseamnă adaptarea strategiilor de război la starea de pace, integrarea funcţiilor O.I. Într-un mediu multinaţional fiind o adevărată provocare.

În ultimii ani, în unele state membre N.A.T.O., operaţiile informaţionale au devenit un concept doctrinar dezvoltat. Deşi nu este acceptat în întregime de alte ţări, acesta reflectă nevoia de a surprinde aspectele unui fenomen care merge dincolo de conceptele tradiţionale de război.

O.I. este o strategie integrată care răspunde la noi vulnerabilităţi şi creează, în acelaşi timp, noi oportunităţi. El introduce în discuţie acele elemente nemilitare ale puterii, cum ar fi: politicile, relaţiile internaţionale, finanţele, infrastructura, percepţia

REPERE CONCEPTUALE

Nu există o definiţie universal acceptată care să acopere întreg conţinutul conceptului de O.I.

Politica N.A.T.O. referitoare la O.I. afirmă: *„Operaţiile informaţionale sunt acţiuni întreprinse pentru a influenţa factorii de decizie, în conformitate cu anumite obiective politice şi militare, prin afectarea informaţiei şi a proceselor care se bazează pe informaţie”*[61].

În cuprinsul documentului se precizează că: *„Operaţiile informaţionale integrează războiul de comandă şi control cu procesul de consultare politicii, cu aparatul de luare a deciziei şi cu operaţiilepolitico-militare ale Alianţei* (...)”. De asemenea, (...) *schimbarea operaţională importantă constă în concentrarea pe rolul informaţiei. Acest lucru include aspectele de percepţie, ca şi pe cele*

61 Citat extras din documentul Comitetului militar MC-422, 15 decembrie 1998, aprobat de Consiliul Nord Atlantic pe 22 ianuarie 199()

tehnice. Planificarea militară nu necesită numai implicarc directă a aparatului politic de luare a deciziei, dar şi o implicare şi o integrare mai largă a unor elemente din conducerea militară”

În context multinaţional, dar la nivelul trupelor de uscat',6\ americanii definesc operaţiile informaţionale ca fiind: *operaţii militare permanente în cadrul mediului informaţional care dau posibilitatea, întăresc şi protejează abilitatea forţei aliate de n culegef procesa şi utiliza informaţia pentru a obţine avantaj faţa de toate categoriile de operaţii militare*”. Se mai afirmă că acestea presupun *„exploatarea capacităţilor de informare şi decizie ale adversarului sau chiar sabotarea acestuia în procesul de luare a deciziilor*; *prin împiedicarea accesului său la informaţii”ă*

O definiţie americană mai recentă, figurând în „Doctrina integrată a operaţiilor informaţionale'466 arată că acestea *„reprezintă acţiuni desfăşurate în scopul afectării informaţiilor şi sistemelor informaţionale ale adversarului, concomitent cu protejarea propriilor informaţii şi sisteme* informaţionaleLectura documentului permite constatarea că aceste operaţii necesită integrarea strânsă şi continuă a capacităţilor şi acţiunilor ofensive şi defensive, precum şi o proiectare, integrare şi interacţiune eficientă a sistemelor de comandă-control, cu sprijinul asigurat de activitatea de informaţii.

Strategii ruşi susţin că operaţiile informaţionale sunt „o *cale de rezolvare a unui conflict dintre două părţi. Scopul este că una dintre părţi să câştige şi să păstreze avantajul informaţional asupra celeilalte. Acest lucru poate fi realizat prin exercitarea unei influenţe informaţionale/psihologice şi tehnice specifice, prin sistemele naţionale de luare a deciziei prin intermediul populaţiei, prin structurile sale informaţionale, ca şi prin înfrângerea sistemului de control al duşmanului, a structurilor sale informaţionale cu ajutorul unor mijloace suplimentare, precum armele, materialele nucleare*”[62].

62 „A Russian View of Future War: Theory and Direction", The

Reflectând asupra acestor definiţii trebuie subliniat faptul că, deşi diferă, au totuşi şi unele elemente comune.

În primul rând, trebuie avută în vedere informaţia. Informaţia se aseamănă mai degrabă unui bun.

Informaţia, ca dimensiune centrală a competiţiei şi a conflictului, ar trebui să ocupe „*linia întâi*” în organizarea arhitecturii sistemului naţional de apărare şi ar trebui să devină, în percepţia liderilor politico-militari, o dimensiune egală, cel puţin, cu cea terestră, aeriană şi maritimă.

În al doilea rând, trebuie să ne referim la sistemele (structurile) informaţionale, prin care se înţelege totalitatea infrastructurilor, organizaţiilor, personalului şi componentelor care realizează culegerea, prelucrarea, stocarea, transmiterea, afişarea şi diseminarea informaţiilor, precum şi acţiunile care au loc ca urmare a informaţiilor obţinute. De reţinut că sistemele informaţionale includ şi procesele orientate către informaţii.

În al treilea rând, trebuie luat în calcul conceptul de superioritate informaţională. Prin acesta se înţelege *„capacitatea de a culege, procesa şi disemina un flux continuu de informaţii, în timp ce este exploatată sau chiar interzisă abilitatea adversarului de a face acelaşi lucru „*

Nu în ultimul rând, trebuie vorbit despre factorii de decizie. În literatura de specialitate, acest concept de influenţare a factorilor de decizie, direct sau indirect, mai poartă şi numele de „război de percepţie” sau „război neocortical”.

DELIMITĂRI SI DIFERENTE

Înţelegerea locului şi rolului actual al operaţiilor informaţionale, la orice nivel (politic, strategic, tactic etc.) şi în tot spectrul de situaţii (pace, criză, conflict etc.), impune stabilirea unei distincţii între acest concept şi cele de *9frăzboi informaţional*” *şi ttrăzboi de comandă-control*”

În sens strict militar, războiul informaţional reprezintă *„operaţii informaţionale desfăşurate în perioade de criză sau de conflict, în scopul atingerii unor obiective*

sau influenţării unor anumite ţinte”[63].

Războiul de comandă-control are, potrivit N.A.T.O.[64], următoarea înţelegere: *folosirea integrată a tuturor capacităţilor militare, inclusiv a operaţiilor de securitater inducerii în eroare, operaţiilor psihologice, războiului electronic şi distrugerii fizice, sprijinite de către sursele de intelligence şi sistemele de comunicaţii şi informatică, pentru interzicerea accesului la informaţie, influenţarea, degradarea sau distrugerea capacităţn de comandă-control a unui adversar; în timp ce toate acestea sunt protejate împotriva unor acţiuni* similareCu alte cuvinte, războiul de comandă-control înseamnă exact ceea ce afirmă şi denumirea sa, executarea de acţiuni pentru prevenirea controlului adversarului asupra informaţiei necesare, pentru realizarea de evaluări şi decizii corecte.

Din formulările oficiale N.A.T.O. se desprinde mai greu diferenţa dintre conceptul mai vechi de război de comandă-control (1996) şi cel de operaţii informaţionale, recent adoptat (1999).

Cu toate că ambele se concentrează pe comandă-control, există o serie de elemente care le deosebesc.

Primul este legat de dependenţa crescândă a organizaţiilor militare de tehnologia informaţională şi de comunicaţii. O mare parte din calitatea activităţilor de comandă-control depinde de calitatea datelor, de receptarea lor în timp util, de software-ul implementat în sisteme de tip C*I (Comandă, Control, Comunicaţii, Calculatoare, Informaţii) etc. Există acum noi mijloace de manipulare şi de distrugere a acestor facilităţi. Aşa cum este definit, războiul de comandă-control nu ia în calcul panoplia *„armelor informaţionale*”[65]: software-ul malign

---

63 „Report of Institute for Strategic Studies, National Defense University, Washington, 1999

64 Definit în documentul Comitetului militar MC-348, „Politica războiului de comandă-control", aprobat de Consiliul Nord-Atlantic în 1996.

65 V. Păun, „Excurs în spaţiul de conflict informaţional", Strategii XXI, nr.2/1997, Bucureşti.

(viruşi, bombe logice, troieni, viermi), microcomponentele cu surprize, armele cu puls electromagnetic, microbii electronici (non-software) şi, nu în ultimul rând, sistemele de suport decizional.

Al doilea element ar fi cel legat de faptul că operaţiile informaţionale nu se limitează doar la vremuri de criză sau conflict.

Un alt element este legat de conceptul de coordonare. Războiul de comandă-control necesită folosirea integrată a cinci acţiuni militare principale: războiul electronic, operaţiile psihologice, inducerea în eroare, securitatea operaţiilor şi distrugerea fizică. Aceşti cinci piloni sunt discipline individuale, iar atunci când există coordonare şi sprijin ferm din partea *intelâigence-ului şi* a comunicaţiilor, întregul pe care ei îl produc – războiul de comandă-control – este mult mai mare decât suma tuturor părţilor.

Prin folosirea celor cinci piloni şi a altor capacităţi militare într-o manieră coordonată, se obţine o sinergie care permite acţiunea eficientă în cadrul unei crize/conflict.

Practic, războiul de comandă-control reprezintă aplicarea militară a operaţiilor informaţionale.

Operaţiile informaţionale nu înlocuiesc războiul de comandăcontrol, ci integrează această „strategie militară” în procesul de consultare politică, în aparatul de luare a deciziei şi o combină cu operaţiile politice şi militare.

Noutatea constă în viteza şi agilitatea operaţiilor solicitate de era electronică, transparenţa mediului operaţional, relativa „dispariţie a distanţei”, natura tot mai efemeră a puterii etc. De asemenea, este nouă estomparea conceptelor „nivel strategic”, „operaţional” şi „tactic”. Viteza comunicaţiilor, diminuarea rolului distanţei şi, în general, natura mult mai transparentă a mediului de conflict sunt împreună sursa acestei estompări. Mai mult, conceptele a ceea ce constituie „zona de operaţii”, „zona de influenţă” şi „zona de interes” ale comandantului îşi măresc semnificaţia datorită tehnologiei de calcul şi

lărgirii câmpului de luptă la ciberspaţiu.

FORMELE DEFENSIVE ŞI OFENSIVE ALE OPERAŢIILOR INFORMAŢIONALE

Există două categorii principale de operaţii informaţionale: operaţiile informaţionale defensive şi operaţiile informaţionale ofensive.

Conform documentelor N.A.T.O., *„operaţiile informaţionale defensive integrează şi coordonează politicile, procedurile, acţiunile, personalul şi tehnologia, pentru protejarea şi apărarea informaţiilor şi sistemelor informaţionale”*[66] şi conţin următoarele elemente:

Siguranţa informaţională – protejează şi apără informaţia prin asigurarea disponibilităţii, integrităţii, autenticităţii, confidenţialităţii şi imposibilităţii ignorării ei. Include măsurile necesare pentru restabilirea funcţiilor vitale ale sistemelor informaţionale prin încorporarea unor capacităţi de protecţie, detectare şi reacţie la atacuri. Utilizează tehnologii şi proceduri de securitate la niveluri multiple, de control al accesului, de securizare a echipamentelor şi de descoperire a acţiunilor cu caracter intru siv.

Securitatea informaţională asigură protecţia şi apărarea sistemelor informaţionale împotriva accesului neautorizat, a modificărilor conţinutului informaţiilor aflate în faza de stocare, prelucrare sau tranzit şi împotriva interzicerii accesului utilizatorilor autorizaţi către aceste informaţii, înglobează, după standardul N.A.T.O., securitatea calculatoarelor (COMPUSEC) şi securitatea comunicaţiilor (COMSEC).

Securitatea operaţiilor – reprezintă procesul de identificare a informaţiilor de importanţă critică, de analizare a activităţilor proprii care pot fi observate de către sistemul informativ al (în)amicului, a indicaţiilor pe care acest sistem le-ar putea obţine, corela şi interpreta, pentru a obţine informaţii de importanţă critică. Totodată, reprezintă procesul de alegere şi executare a acelor

66 Definiţie figurând în documentul Comitetului Militar N.A.T.O. MC- 422 „Information Operation Policy", 22.01. 1999

măsuri care să elimine sau să reducă, la un nivel acceptabil, vulnerabilităţile în faţa acţiunilor (în)amicilor.

Contrainducerea în eroare – sprijină acţiunile defensive prin eliminarea, neutralizarea sau diminuarea efectelor generale ale acţiunilor de inducere în eroare ale (în)amicilor sau prin exploatarea efectelor generate de acestea.

Contrapropaganda – are ca scop demascarea încercărilor (în)amicilor de a desfăşura acţiuni de propagandă şi a scopurilor acestora.

Acţiunile de contrainformaţii – contribuie la desfăşurarea cu succes a operaţiilor informaţionale defensive prin furnizarea de informaţii şi prin desfăşurarea de activităţi care să protejeze informaţiile proprii împotriva spionajului, sabotajului sau acţiunilor teroriste.

Războiul electronic – protecţia prin mijloace electronice presupune acele acţiuni care vizează minimalizarea efectelor folosirii mijloacelor electromagnetice. Sprijinul prin mijloace electronice contribuie la realizarea cu succes a avertizării, prin descoperirea, identificarea şi localizarea surselor de energie electromagnetică ce pot constitui ameninţări.

Relaţiile publice – contribuie la siguranţa informaţională prin difuzarea de informaţii, care descriu fapte şi situaţii, în scopul contracarării acţiunilor de inducere în eroare şi de propagandă ale (în)amicilor.

Securitatea fizică – urmăreşte asigurarea unui grad de protecţie fizică a infrastructurii informaţionale şi a unor capacităţi de reacţie în cazul detectării atacurilor.

În concluzie, operaţiile informaţionale defensive se concentrează pe protecţia propriei informaţii, a proceselor bazate pe informaţie, a sistemelor de comandă-control şi a celor de comunicaţii şi informatică. Această protecţie trebuie să fie adaptată pentru orice tip de (în)amic, în orice situaţie (pace, criză, conflict) şi vizează patru componente: protecţia infrastructurii informaţionale, descoperirea atacurilor, restaurarea funcţiilor vitale şi reacţia la atacuri. Integrarea tuturor componentelor enumerate este

esenţială.

Operaţiile informaţionale ofensive implică folosirea integrată a capacităţilor şi activităţilor desemnate, sprijinite de activitatea informativă (*itelligence*), cu scopul de a afecta factorii de decizic (în)amici şi de a promova obiective specifice.

Capacităţile folosite în acest scop includ (dar nu se limitează numai la ele) următoarele elemente:

Operaţiile psihologici – sunt destinate transmiterii anumitor informaţii şi indicaţii către exterior, în scopul influenţării atitudinilor, motivaţiilor, raţionamentelor şi, în final, a comportamentului altor entităţi. Pot lua forma unor poziţii exprimate la nivel politic sau diplomatic, unor comunicate, anunţuri, difuzării de broşuri, manifeste, emisiuni de radio şi T.V. etc.

Inducerea în eroare – vizează factorii de decizie prin afectarea proceselor şi sistemelor de culegere, analiză şi difuzare a informaţiilor de către (în)amici. Acest lucru presupune cunoaşterea detaliată a (în)amicilor şi a proceselor decizionale ale acestora. Hlementul cheie îl constituie anticiparea. Acţiunile de inducere în eroare depind de modul de desfăşurare a acţiunilor de asigurare informativă, în scopul identificării celor mai potrivite ţinte pentru elaborarea unui scenariu credibil şi pentru aprecierea eficacităţii planului de inducere în eroare.

Războiul electronic presupune acţiuni destinate distrugerii, neutralizării sau degradării capacităţilor electronice ale (în)amicilor sau reducerea capacităţii acestora de a utiliza în mod eficient spectrul electromagnetic. Protecţia şi sprijinul prin mijloace electronice reprezintă exemple de capacităţi care contribuie la promovarea şi îndeplinirea unor obiective specifice.

Relaţiile publice – pot contribui la desfăşurarea operaţiilor informaţionale ofensive prin difuzarea de informaţii corecte şi oportune către auditoriul intern (propria organizaţie) şi extern (publicul larg), prin informarea despre scopurile, posibilităţile şi intenţiile

dorite. Documente oficiale precizează că *activităţile de relaţii publice nu sunt folosite ca modalităţi de inducere în eroare sau ca modalităţi de dezinformare a auditorului intern sau extern „*[67].

Atacul fizic/distrugerea – se referă la folosirea mijloacelor de distrugere asupra ţintelor informaţionale, ca element component al efortului integrat reprezentat de operaţiile informaţionale.

Relaţiile ci vi li-militari – cuprind, în viziunea N.A.T.O., *„totalitatea activităţilor prin care factorii de decizie stabilesc şi dezvoltă relaţii între forţele proprii şi autorităţile civile, resursele şi instituţiile din zonele amice, neutre sau inamice în care sunt desfăşurate aceste forţe”*[68].

Scopul de bază al operaţiilor informaţionale ofensive este de I influenţa cunoştinţele şi credinţele factorilor de decizie, pentru a le reduce voinţa şi abilitatea de a decide şi pentru a perturb; procesul decizional.

MANAGEMENTUL PERCEPŢIILOR ŞI FACTORUL UMAN

Adevărul nu este doar ceea ce crezi că este, ci el rezidă în circumstanţele în care este spus, cui, de ce şi cum este spus.

Vaclav *Havel*

Un aspect distinct al operaţiilor informaţionale ofensive îl constituie managementul percepţiei, proces care cuprinde discipline precum relaţiile publice, diplomaţia publică, operaţiile psihologice (PSYOPS), inducerea în eroare şi acţiunile sub acoperire.

Managementul percepţiei ţinteşte dimensiunea umană în politică şi în situaţii de conflict, într-un mod în care armele fizice nu o pot face. Acesta este înţeles ca proces care determină acele acţiuni ce transmit şi/sau împiedică accesul adversarilor la informaţie, pentru a influenţa emoţiile, motivele sau obiectivele lor, vizându-se, în final, materializarea acestora în comportamente şi

67 MC 402 N A.T.O., Psyhological Operations Policiy", 07.04.1997
68 MC 411 N.A.T.O., Civil-Milytary Operations Policiy", 1998

acţiuni favorabile iniţiatorilor.

Diplomaţia publică este menită să convingă diferite audienţe asupra adevărului şi raţionalităţii politicii, intenţiilor şi acţiunilor unei alte entităţi. În general, diplomaţia publică funcţionează pe căi tradiţionale – dialog diplomatic şi politic direct, conferinţe de presă, comunicate de presă, interviuri ete. — dar viteza la care se desfăşoară astăzi unele evenimente cere capacităţi de comunicare pe măsură. Liderii unor puteri mici sau actorii non-statali au în prezent la dispoziţie posibilităţi de informare la fel de sofisticate ca şi cele deţinute de liderii marilor puteri. Poate cea mai semnificativă diferenţă faţă de trecut este faptul că oamenii au nevoie să fie conectaţi la tot ce se întâmplă pe întreg mapamondu I

Aceasta înseamnă o multiplicare a surselor şi un acces cât mai rapid posibil.

O diplomaţie eficientă, care contribuie prin mijloacele sale specifice la „modelarea spaţiul informaţional”, necesită luarea simultană în considerare a diverselor surse de informare, mesajelor transmise şi audienţei vizate.

Inducerea în eroare acţionează diferit faţă de celelalte elemente ale managementului perccpţiei. Dacă relaţiile publice, diplomaţia publică şi majoritatea formelor de operaţii psihologice caută să informeze şi să convingă într-o manieră corectă, inducerea în eroare dimpotrivă, distorsionează deliberat sensul realităţii pentru adversarul declarat.

Legăturile implicite existente între PSYOPS şi inducerea în eroare creează adesea confuzii din cauza lipsei familiarităţii cu cele două discipline. PSYOPS sunt caracterizate ca fiind „albe” „gri” sau „negre”, în limbajul de specialitate, însă acest aspect nu se referă la conţinutul de adevăr al mesajelor, ci mai de grabă la identitatea sursei: adevărată, neidentificată sau falsă. Dar, indiferent de sursă, scopul PSYOPS este de a furniza ţintei acea informaţie reală şi credibilă care să determine comportamentul dorit. Inducerea în eroare poate

îmbunătăţi furnizarea mesajelor către ţintă prin folosirea unor informaţii reale şi verificabile, ceea ce va spori credibilitatea mesajului, dar metodele folosite şi informaţiile transmise sunt de altă factură decât cele utilizate în PSYOPS.

Cu toate acestea, linia de demarcaţie dintre PSYOPS şi inducerea în eroare este deseori greu de perceput, cele două discipline sprijinindu-se reciproc în practică.

Înţelegerea culturală a audienţei-ţintă este un element critic în realizarea credibilităţii. Un mesaj devine cu atât mai credibil cu cât este mai corect cultural, indiferent dacă este adevărat sau fals. Tehnologia disponibilă astăzi permite personalizarea mesajelor în funcţie de ţintă şi de modul agreat de ea în receptare. Nu mai contează dacă mesajul este adevărat sau fals, dacă el este ambalat şi transmis corespunzător. Folosirea canalelor directe pentru distribuirea mesajelor poate, de asemenea, să sporească credibilitatea acestora. Pe acest fapt se bazează succesul inducerii în eroare, care preferă această cale de distribuire a mesajelor, în cazul PSYOPS este indicat ca unele mesaje să fie transmise şi pe alte canale, dar nu în mod obligatoriu. Acest fapt se dovedeşte util, deoarece credibilitatea mesajelor depinde şi de capacitatea adversarului de a verifica conţinutul lor şi pe alte căi decât cele anticipate. Realizarea unui nivel similar de credibilitate pentru mesajele destinate inducerii în eroare este mult mai dificil de realizat tocmai pentru că mediul informaţional de azi permite ţintei verificări multiple ale acestora.

Rezultatele experienţei câştigate în urma conflictelor din ultimul deceniu, din perspectiva PSYOPS, au determinat recunoaşterea acestora ca fiind o componentă importantă a planificării operaţiilor militare. În ultimul timp, PSYOPS suni recunoscute de planificatorii militari ca fiind un ingredient absolul necesar în ceea ce se numeşte „*invitational opérations*” unde cerinţa de bază a îndeplinirii misiunii o reprezintă consensul popular (de exemplu, operaţiile umanitare sau de menţinere a păcii).

Diferitele elemente constitutive ale managementului percepţiilor nu pot fi implementate corespunzător în practică în afara capacităţilor de a înţelege (şi în final de a ţinti) modul de asimilare şi procesare a informaţiilor de către oponenţi. Prin monitorizare continuă, dinamică şi prin ţintirea focalizată a sistemelor de informaţii (computerizate sau nu) ale (în)amicului se obţin cunoştinţe detaliate despre infrastructura fizică şi interrelaţională ce înconjoară ţinta. Analiza factorului uman necesită construcţia unui tablou general al mediului informaţional care înconjoară ţinta, precum şi un tablou general al infrastructurii umane, a statului ţintă sau a unei anumite organizaţii (grup) ţintă.

Prin analiza factorului uman se înţelege un cumul de elemente psihologice, culturale, comportamentale precum şi alte atribuie

Umane care influenţează luarea unei decizii sau a informaţiilor pe care le deţine o persoană şi interpretarea individuală sau de grup a acestora. Analiza factorului uman are un rol cheie în desfăşurarea operaţiilor de-management al percepţiilor.

Ea se axează în principal pe trei tipuri de elemente existente sau potenţiale ale sistemelor adversarului:

autoritatea factorilor de decizie structurile naţionale sau de grup implicate în luarea deciziei procesul decizional în sine

Analiza acestor elemente presupune elaborarea unui studiu detaliat al naturii şi caracteristicilor regimurilor analizate sau a grupului ţintă. Prin aceste analize trebuie înţelese locul, intensitatea şi expunerea factorilor externi, de mediu, factori care pot influenţa procesul decizional şi acţiunile liderilor sau grupurilor.

Urmărirea, analiza şi evaluarea aspectelor pur psihologice teprezintă cheia analizei factorului uman. În acest tip de analiză se ţine cont şi de faptul că anumite elemente culturale ale sistemelor decizionale analizate implică şi înţelegerea complexului istoric şi a influenţelor manifestate de-a lungul secolelor.

Astfel, un anumit tip de regim va genera un tip specific de (Comportament în luarea deciziilor. Acest fapt implică obligatoriu finalizarea atât a caracteristicilor sociale care includ aspecte demografice, lingvistice, componenţă etnică, influenţe naţionale şi sub-naţionale, cât şi impactul pe care îl are geografia asupra naturii şi culturii unui popor.

Studiul conducerii presupune înţelegerea detaliată a unei arii foarte largi de probleme cum ar fi:

Înţelegerea personalităţii intrinseci şi a temperamentului liderilor politici, militari etc;

analiza şi interpretarea obiectivelor generale şi specifice îşi aspiraţiile urmărite în mod individual sau a celor de grup;

Înţelegerea credinţelor, sistemelor de valori şi a tendinţelor ţintelor vizate Între o organizaţie de tip birocratic, structurată ierarhic şi un grup terorist, de exemplu, nu numai diferenţele culturale sunt importante, ci şi structurile relaţionale din interiorul acestora. Acestea vor face în mod special obiectul analizei factorului uman.

Prin acest tip de analiză pot fi anticipate acţiunile individuale ale decidenţilor (ceea ce oferă posibilitatea ameliorării sau îmbunătăţirii propriilor O.l), dezvoltarea lor profesională, stilul decizional al conducerii, pe scurt, un întreg profil psihologic şi o întreagă evaluare a (în)amicului.

ELEMENTE ALE UNEI STRATEGII DE INFLUENŢARE

Schimbarea este o lege a firii. Cei care privesc doar spre trecui sau doar spre prezent vor rata, cu siguranţă, viitorul.

John F. Kennedy

Exportată intens de S.U.A., dar greu de digerat pentru mulle din statele europene membre N.A.T.O., revoluţia în afacerile militare (R.A.M.) implică pentru o ţară ca România, o schimbare de paradigmă în gândirea şi practica strategică, dificilă în context u I actual, în care politicile structuraliste de reformă şi modernizare a

sistemului de siguranţă naţională sunt, în esenţă, de natura energetică.

Necesitatea unui proces de tip R.A.M., în cadrul sistemului de siguranţă naţională al României în anii următori, trebuie motivată de o viziune strategică de ansamblu, comună cu cea euro atlantică.

Dar cum poate fi creată o astfel de perspectivă când Statele Unite şi Europa au viziuni destul de diferite?

Care va fi modelul strategic de urmat?

Asimetria dintre strategia militară, capacităţile şi tehnologia S.U.A., pe de o parte, şi partenerii săi militari, aliaţii N.A.T.O de cealaltă parte, constituie un motiv de preocupare pentru tot mai mulţi analişti politico-militari şi lideri politici. Înţelegere;

acestei diferenţe este importantă pentru România în procesul de integrare euro-atlantică.

Temeiuri şi polemică

Din perspectiva asimetrii lor şi tendinţelor de bipolarizare ale sistemului euro-atlantic de securitate este dificil, cel puţin în etapa actuală, a se decide asupra modelului strategic de aplicat în continuarea reformei (cu toate că, în practică, abundenţa de date şi oferta de know-how fac mai atractiv şi uşor de adoptat modelul american).

Un start adaptat şi adecvat în R.A.M. Înseamnă promovarea unui comportament politico-militar proactiv (strategia acţiunii), utilizând instrumente de analiză, instruire şi sprijin decizional (strategia optimalităţii) şi desfăşurând acţiuni de protejare şi influenţare a informaţiilor, proceselor şi sistemelor informaţionale proprii, ale (în)amicilor (strategia de influenţare), prin operaţii informaţionale.[69]

Având un rol de descurajare, în absenţa altor elemente credibile, strategia acţiunii trebuie să permită creşterea, după împrejurări, a puterii sau a influenţei ţării în exterior. Aceasta presupune o reînnoire simultană a

69 Diferenţa nu rezidă neapărat într-un accent pus diferit pe tehnologia informaţională, ci este mai mult o chestiune de paradigmă.

strategiei directe, în care forţa armată joacă rolul cel mai important şi a strategiei indirecte în care, fără a fi exclusă, forţa armată se află într-un plan secundar.

Strategia acţiunii este stimulată de apariţia unor operaţii noi la nivel strategic, al căror scop nu este în esenţă hotărât pe calea armelor sau a confruntării fizice şi care se înscriu în mai multe strategii indirecte. Acest aspect antrenează în fapt o diversitate de „câmpuri de operaţie”[70] în care trebuie să se desfăşoare angajamentele.

În noul context, determinarea capacităţilor strategice necesare şi planificarea siguranţei naţionale trebuie să înceapă printr-o analiză a câmpurilor de operaţie în care acestea pot acţiona cu eficacitate.

Analiza invită la redimensionarea conceptului clasic de „operaţie” dincolo de limitele geografice impuse de conţinutul său tradiţional: „zonă de operaţii”, punând în discuţie inclusiv limitele temporale.

Strategia optimalităţii. În contextul actual de redimensionarc şi optimizare a structurilor de siguranţă, lansarea procesului de dezvoltare consistentă şi pragmatică a domeniului modelaresimulare apare ca o necesitate fezabilă.

Prin componentele sale fundamentale (modelele, simularea în teren, jocurile de război şi politici militare, simularea virtuală), acest domeniu poate fi unul dintre pilonii procesului de modernizare şi reformă şi, totodată, poate asigura o optimizare a proceselor şi activităţilor specifice structurilor care au atribuţii în domeniul siguranţei naţionale a României.

De asemenea, prin utilizarea efectivă a instrumentelor de analiză şi sprijin decizional, maniera de rezolvare a problemelor de orice natură şi palier ierarhic poate fi îmbunătăţită, dând posibilitatea factorilor de

---

70 Confonn unei tipologii prezentate de Felix Faucon, câmpurile operaţionale se împart în câmpuri conceptuale, psiho-sociologice, geppolitice, geografice, fizice câmpuri ale sistemelor de decizie şi de Informaţie („Guerre de lp—infonnation ou opérations d'infonnàtion?", Defense Naţionale, nr. 3, 1998).

decizie să evite concentrarea asupra rezolvării crizelor imediate şi să se îndrepte spre o stare de anticipare a evenimentelor.

Strategia optimalităţii trebuie corelată cu o politică dinamică de dezvoltare a infrastructurii informaţionale naţionale, al cărei accent să cadă pe protejarea infrastructurii critice şi pe deplasarea priorităţilor spre zona informatică a serviciilor de informaredocumentare, sinteză şi fuziune a cunoştinţelor.

Strategia de influenţare. Evenimentele ultimului deceniu pol sugera desfăşurarea unor subtile operaţii informaţionale în spaţiu I geostrategic de interes al României.

Principalele caracteristici ale reacţiilor la aceste acţiuni au fost, din diverse cauze, unilateralitatea ripostei, lipsa de coordonare şi absenţa unei viziuni globale, integratoare. Unul din cele mai mari pericole este acela că, uneori, probabil nici nu s-a conştientizat faptul că factorii de decizie au fost ţinta unor astfel de acţiuni. Există, de asemenea, un risc al,Interoperabilität" care se poate formula astfel: cine are o cunoaştere foarte bună despre arhitectura sistemelor de comunicaţii şi informatică, substanţa deciziei şi transformările logice dintr-un sistem de conducere ar putea determina transformările dorite.

Totodată, în ultimii ani, în „spiritul interoperabilitaţii", au fost importate diverse concepte şi modele militare occidentale, într-un mod destul de artificial, fără o înţelegere şi adecvare de profunzime şi, în consecinţă, cu un succes discutabil.

Ansamblul orientărilor şi deciziilor în materie de reformă a organismului militar, necesită, dincolo de procesul cunoscut sub numele „Military Action Plan", de standardele deja clasice de interoperabilitate, de strategia de imagine etc., o aliniere şi adecvare la „schimbările de fond ale naturii conflictelor".

Strategia de influenţare presupune dezvoltarea adecvată a domeniului „operaţii informaţionale" pentru a se ajunge, la nivel naţional, la stadiul în care să se dispună

de un cadru legislativ şi metodologic, precum şi de un ansamblu de structuri şi mijloace specializate, capabile să descurajeze pe căi şi prin mijloace informaţionale acţiunile contrare intereselor naţionale, să contracareze efectele acţiunilor informaţionale la nivelul factorilor de decizie şi al sistemelor informaţionale.

În concluzie, interesul pentru”noua cultură a conflictelor” şi „revoluţia informaţională” – cu determinări majore privind extinderea responsabililăţilor organismului militar în materie de siguranţă naţională, proiectarea unor capacităţi strategice şi redefinirea proceselor de comandă şi control din perspectiva asimetriei – reclamă o luare în considerare a următoarelor aprecieri, care. integrale, construiesc un posibil cadru teoretic general de reflecţie:

„Utilizarea forţei în mod eficient, pe o scară mai mare sau mai mică, se face mai mult pentru a preveni escaladarea conflictelor decât pentru o confruntare directă de forţe militare.”[71]

„Orice conflict poate fi tolerat dacă nu produce victime omeneşti” – aserţiune susţinută de teoria campaniilor informaţionale.

Trecerea de la un concept clasic de organizare la unul postmodern presupune „schimbarea caracterului forţelor armate, care nu trebuie să mai reprezinte expresia – naţiune în armată – ci să fie mai degrabă un corp de profesionişti.”[72]

Tehnologiile informaţionale, ca o condiţie pentru acţiunea militară eficientă, sunt dimensiuni esenţiale în planul evoluţiei gândirii şi practicii militare. Pe măsură ce aceste tehnologii se schimbă, se schimbă şi contextul în care sunt făcute alegerile de politică, strategie şi doctrină

---

71 E. Luttwak, „The Crisis of Classic Military Power & the Possible Remedy of Post-Heroic Intelligence-Based Warfare", The Information Revolution & International Securtfy, Center for Strategic & Internationa l Studies, 1998

72 R.Jervis, „Signaling / Perception in the Information Age", The Information Revolution & National Security, Strategic Studie. Institute, 2000

militară. Pe măsură ce sunt elaborate noi tehnologii, se modifică şi sfera alternativelor posibile privind planificarea apărării şi acţiunea militară propriu-zisă.

Revoluţia informaţională oferă tehnologii care modifica continuu influenţa binomului timp-spaţiu şi contribuie substanţial la creşterea complexităţii; transformă liniarul în neliniar şi secvenţialul în simultan. Teoria complexităţii şi nelimaritatea (viziunea neo-clausewitziană) – generatoarea unei noi paradigme în gândirea militară – impun o reconstrucţie a mediului militar.

Noua cultură a conflictelor contribuie la consolidarea curentului centrat pe filosofia lui Sun Tzu: gândire simplă, bazată pe inducere în eroare şi cunoaşterea minţii (în)amicului. Principiile lui Sun Tzu, puse în acord cu elementele tehnologice, pun bazele unei noi strategii de competiţie/negociere şi de rezolvare a crizelor.

Următoarele afirmaţii încearcă să contureze (sau mai mult să sugereze) un cadru general de abordare a problematicii „operaţiilor informaţionale”:

Există, în prezent, posibilităţi de influenţare a politicii diferitelor entităţi (state, actori transnaţionali, organizaţii, indivizi etc.), fără a se folosi forţa armată. Există forme de conflict în care războiul convenţional este marginal, dacă nu chiar absent. Definiţia clausewitziană a războiului se erodează treptat. „Operaţiile informaţionale” devin posibilităţi din ce în ce mai atractive de promovare şi menţinere a intereselor (naţionale, organizaţionale, individuale etc.).

Conflictele sunt mai mult decât „ciocniri de tehnologie”. Supremaţia tehnologică nu a putut împiedica nici înfrângerea Olandei în Indonezia, a Franţei în Indo-China şi Algeria, a Americii în Vietnam, a Uniunii Sovietice în Afganistan, a Rusiei în Cecenia şi nici asigura succesul N.A.T.O. În Kosovo. Aceste episoade confirmă faptul că superioritatea tehnologică nu este o garanţie implicită a victoriei pe câmpul de luptă, şi cu atât mai puţin la masa negocierilor. Tehnologia este importantă, dar nu decisivă.

Vrând-nevrând, globalizarea şi „societatea informaţională” devin realităţi presante, generatoare de forme noi de agresiune (informaţională), cu implicaţii în redefinirea conceptului de securitate naţională (prin adăugarea unei dimensiuni noi – „securitatea informaţională”[73]).

Dacă „societatea informaţională” – spre care ne îndreptăm – este un factor major de generare a prosperităţii şi o cerinţă vitală pentru integrarea europeană, atunci „securitatea informaţională” reprezintă un factor-cheie pentru protejarea intereselor naţionale.

Acesta este un alt motiv pentru care trebuie să vorbim de război şi operaţii informaţionale.

Este evident, de asemenea, că spectrul actual al crizelor şi conflictelor include, pe lângă spaţiul fizic, obişnuit nouă, şi spaţiul virtual.[74] Trebuie să ne pregătim să facem faţă amândurora, pentru că spaţiul virtual este o cale importantă pentru o entitate mai mică de a-şi crea o contrapondere în faţa unor entităţi mai mari sau/şi mai avansate din punct de vedere tehnologic. Totodată, spaţiul virtual este o soluţie complementară viabilă de management al riscurilor la adresa siguranţei naţionale.

Nu în ultimul rând, a vorbi despre necesitatea utilizării operaţiilor informaţionale – ca factor de descurajare la nivel strategic şi catalizator către un comportament politico-militar proactiv – presupune conştientizarea faptului că primul pas în direcţia unei deschideri trebuie să îl reprezinte spargerea rezistenţei la schimbare.

---

73 Prin securitate informaţională se înţelege „starea de protecţie a necesităţilor de natură informaţională ale individului, societăţii şi statului, care să permită asigurarea satisfacerii acestora şi evoluţia lor progresivă, independent de prezenţa ameninţărilor de natură informaţională, interne şi externe", http/www.ndu.edu/inss/siws/ eont.html

74 Obişnuinţa cu (in)amici şi/sau competitori bine conturaţi generează pericolul ignorării acelora care se manifestă în spaţiul virtual

Inserarea de noi paradigme (O.I. de exemplu) în procesul complicat şi sinuos al modernizării este importantă, deoarecc acestea sunt acţiuni şi instrumente absolut necesare în stabilirea condiţiilor, planificarea şi conducerea eforturilor în domeniul siguranţei naţionale.

O.I. sunt un instrument care asigură un avantaj cert în mediu 1 geostrategic actual – un mediu tot mai dependent de informaţie şi de infrastructură care asigură tipul şi volumul informaţiilor de care este nevoie. Sistemele naţionale de bază (politic, social, economic, militar şi ecologic) depind de informaţie şi de instrumentele informaţionale (comunicaţii, automatizare). Această dependenţă constituie, în egală măsură, putere şi vulnerabilitate. Pe de o parte, dependenţa înseamnă a avea posibilitatea racordării siguranţei naţionale la realităţile occidentale ale „revoluţiei în afacerile militare”[75], având la dispoziţie tehnologie de vârf. Dar, pe de altă parte, aceasta înseamnă vulnerabilitate la atacurile care ar putea provoca efecte dezastruoase la nivelul propriului proces decizional.

O.I., ca modalităţi de acţiune pe timp de pace şi în situaţii de criză şi conflict, reprezintă un punct de plecare radical diferit faţă de prezent şi constituie, într-adevăr, o revoluţie a modului de luptă.

Trebuie luat în calcul şi faptul că există o importantă teorie occidentală în acest domeniu şi chiar o politică N.A.T.O.[76] privind O.I.. Orice viitoare teorie proprie O.I, chiar dacă va adopta sau adapta litera occidentală, prin spiritul său trebuie să ne ajute să percepem corect amploarea transformărilor induse de „revoluţia informaţională”, să înţelegem că trebuie să ne dezvoltăm capacităţi intelectuale şi tehnice adecvate pentru a duce O.I şi să conştientizăm că (în)amicii şi/sau partenerii noştri

---

75 „Revoluţia în afacerile militare" implică folosirea tehnologici informaţionale pentru a obţine superioritatea informaţională, prin cunoaşterea unui spaţiu de conflict, în toate dimensiunile sale, şi prin asigurarea celei mai bune reacţii, la orice nivel.

76 Documentul MC-422 „Information Operation Policy", adoptat la 22.01.1999

vor vedea, cu siguranţă, vulnerabilităţile noastre informaţionale şi vor încerca să le exploateze.

O dezvoltare generală proprie O.I. trebuie să ia în calcul şi să particularizeze cel puţin două teorii – teoria agregării şi teoria neliniarităţii – concepte esenţiale în înţelegerea acţiunilor informaţionale. Teoriâ agregării include interacţiunea lucrurilor (indivizi, organizaţii etc.) şi a legăturilor (elemente fizice, activităţi etc.). Când se combină lucruri şi legături rezultă efecte importante, mult mai importante decât dacă ar fi rămas separate.

Agregarea trebuie studiată din perspectiva integrării unor domenii, discipline şi tipuri de acţiuni distincte în cadrul unei O.I. — acţiunile psihologice, (contra)informaţiile, (contra)inducerea îti eroare, relaţiile publice, relaţiile militari-civili, (contra)acţiunea electronică, securitatea şi siguranţa informaţională, securitatea operaţiilor, securitatea fizică, (contra)propaganda şi acţiunile speciale. Înţelegerea teoriei agregării, modelarea şi simularea proceselor militare din perspectiva neliniarităţii (teoria haosului şi teoria complexităţii), precum şi înţelegerea modului de a crea intenţionat efecte de nivel doi şi trei, toate acestea deschid uşa planificării şi executării unor O.l. care să descurajeze şi să reducă riscurile polilico-militare.

În ciuda gravităţii problemei, suntem, momentan, la începuturile examinărilor teoretice[77], necesare dezvoltării unei teorii şi practici viabile a operaţiilor informaţionale, care să fixeze un cadru instituţionalizal de abordare şi adoptare a unei reacţii politico-militare în situaţii de criză şi conflict specifice epocii informaţionale (dacă acceptăm că mediul geostrategic actual sc îmbogăţeşte cu „trăsături informaţionale”).

CONCLUZII

77 In competiţia pe plan conceptual şi doctrinal-, în raport cu temele de reflecţie majore actuale (teoria neo-clausewitziană a neliniarităliii războiului, modelarea şi simularea acţiunilor militare, operaţiile informaţionale, managementul riscurilor etc.) gândirea militară românească manifestă o inexplicabilă rămânere în urmă.

Rapida evoluţie a tehnologiei informaţiei a dus la o schimbarc de paradigmă privind natura conflictelor. Războiul informaţional este acum o noţiune practică pentru multe naţiuni. Costul necesar pentru obţinerea de capacităţi credibile defensive privind R.I. este relativ scăzut, cu siguranţă mult mai mic decât cel necesar pentru realizarea unei siguranţe naţionale convenţionale. Iată de ce capacităţile în domeniul R.I. sunt o alegere atractivă pentru un spectru larg de entităţi tradiţionale sau modeme.

R.I. are la bază o strategie integratoare care recunoaştc importanţa şi utilitatea informaţiilor în comanda şi controlul sistemului de siguranţă naţională şi în implementarea strategici de securitate naţională. R.I. exploatează oportunităţile şi vulnerabilităţile inerente dependenţei crescânde de informaţie, concentrându-se asupra sistemelor şi tehnologiei informaţionale.

R.I. nu este un fenomen cu care se confruntă doar ţările evoluate. Structura actuală a sistemului internaţional se îndreaptă spre o relaţie de interdependenţă statală tot mai accentuată, în care sunt angrenate atât statele dezvoltale, cât şi cele mai puţin dezvoltate.

Modul de a înţelege şi de a percepe fenomenul R.I. diferă de la o ţară la alta în funcţie de realităţile proprii fiecăreia şi de interesele pe care consideră că le poate promova cu ajutorul acestui instrument.

Trecerea în revistă a câtorva puncte de vedere aparţinând unor state care au preocupări în domeniu!!! lasă să se degajeze cel puţin patru idei comune.

În primul rând, R.I. poate fi înţeles doar în cadrul întregului complex de schimbări. El nu influenţează doar sectorul militar, ci întreaga societate şi comunitate internaţională.

Unul dintre efectele tehnologiei informaţionale este crearea spaţiului virtual, ca o nouă dimensiune în care poate fi dus războiul. Spaţiul virtual are elemente de bază inseparabile: forţele armate, naţiunea şi comunitatea internaţională. Toate nivelurile de comandă şi control pot fi

atacate şi, în consecinţă, trebuie să fie apărate. La toate nivelurile, omul este cel care are puterea de decizie finală. Acest aspect face din conceptul de „influenţă” o opţiune şi un pericol. Statele moderne se confruntă cu o dilemă. Pe de-o parte, digitalizarea este un stadiu evolutiv firesc spre care tind societăţile moderne şi, pe de altă parte, aceste progrese creează noi şi serioase vulnerabilităţi.

În al doilea rând, R.L este o adevărată problemă. El pune sub semnul întrebării o serie întreagă de „vechi adevăruri”. Nu există soluţii uşoare. Un prim pas ar fi înţelegerea faptului că există riscuri. Un alt pas constă într-o evaluare atentă a vulnerabilităţilor. Tehnologia aduce multe foloase, dar şi o mulţime de greutăţi.

În al treilea rând, planificarea şi ducerea unui R.I. strategic este, în orice caz, un proces complex în care, aşa cum este cazul Cu toate formele de război, informaţiile şi serviciile de informaţii sunt un factor-cheie pentru dezvoltarea şi desfăşurarea unor planuri şi operaţiuni efective de R.L, fie pentru dezvoltarea unor măsuri proprii de protecţie a sistemelor militare, fie pentru realizarea unui sistem de degradare a capacităţilor acţionale ale unui (în)arnic.

Nu în ultimul rând, studiile de vulnerabilitate, analizele efectuate pentru caracterizarea ameninţării, simpozioanele internaţionale dovedesc importanţa acordată de comunităţile de informaţii acestui nou fenomen. Deja ameninţarea informaţională nu mai este doar problema specialiştilor din domeniul militar. Mass-media începe să propage efecte devastatoare ale acestei arme noi, prea puţin convenţionale.

R.I. a acordat, de altfel, un plus de autoritate actorilor şi aspectelor netradiţionale. Organizaţiile mici cu buget restrâns, sunt acum capabile de o mai mare agresivitate şi influenţă decât ar li putut prezice teoriile relaţiilor internaţionale.

Din acest motiv, conceptul tradiţional de siguranţă naţională trebuie să evolueze spre ceva mai flexibil, mai proactiv şi mai dinamic. Pregătirea trebuie să vizeze cel

puţin trei niveluri:

politic – să se aibă imaginea de ansamblu a ameninţărilor la adresa infrastructurii informaţionale la nivel naţional şi internaţional;

de *intelligence* – să se înţeleagă indicatorii şi avertizările şi să se poată conlucra cu planificatorii strategici;

de sistem – să se recunoască atacurile şi să se ştie cum să se reacţioneze;

În final, se poate afirma că:

Noua cultură a conflictelor se cristalizează odată cu crearea noii dimensiuni cibernetice şi cu apariţia noilor concepte şi instrumente strategice, printre care operaţiile informaţionale strategice, derulate prin intermediul operaţiilor psihologice complexe, conflictelor mediatice, atacurilor digitale sau managementului percepţiilor.

Strategiile asimetrice centrate pe acţiuni informaţionale defensiv-ofensive nu vor conduce la o forţă de reacţie mult mai puternică în sensul cantitativ clasic, ci mai degrabă la o mai mare abilitate 4e folosire a forţei neconvenţionale pe timp de pace şi în situaţii de criză, pentru menţinerea şi promovarea intereselor naţionale şi chiar la posibilitatea de planificare a mijloacelor clasice într-o mai mare măsură, cu discernământ şi acurateţe. Dacă aceste consideraţii se corelează cu realitatea efortului guvernamental de dezvoltare a societăţii informaţionale, atunci provocările pentru decidenţii şi planificatorii din sistemul siguranţei naţionale de abia acum încep.

Totalitatea operaţiilor informaţionale desfaşurate în timp de criză sau conflict în scopul atingerii unor obiective sau influenţării unor anumite ţinte poartă numele de „război informaţional”.

Războiul de comandă-control este aplicarea în plan militar a operaţiilor informaţionale.

Operaţiile informaţionale pot fi înţelese doar în cadrul întregului complex de schimbări. Ele nu influenţează doar sectorul militar, ci şi întreaga societate şi

comunitate internaţională.

Operaţiile informaţionale nu se confundă cu operaţiile de informaţii, care sunt desfaşurate exclusiv de structurile de informaţii.

Operaţiile informaţionale pot contribui la integrarea elementelor militare ale puterii naţionale cu celelalte elemente, în scopul atingerii obiectivelor naţionale.

Unul dintre cele mai mari câştiguri, ce poate fi exploatat de pe urma folosirii operaţiilor informaţionale, este abilitatea lor de a preveni dezvoltarea unei crize în conflict. În acest sens, operaţiile informaţionale trebuie să fie desfaşurate încă de pe timp de pace şi necesită atât sprijin politic, cât şi militar.

Totodată, operaţiile informaţionale pot fi folosite pentru întreruperea sau chiar ruperea legăturilor de tip social, ţintele fiind transportul, comunicaţiile, energia, instituţiile financiare etc. prin *ţrfolosirea ciberspaţiului*[78], *pentru afectarea operaţiilor militare strategice şi pentru aducerea de prejudicii infrastructurilor informaţionale naţionale*". Un astfel de atac asupra societăţii poate avea consecinţe foarte grave. În acest context, nu este deloc surprinzător faptul că multe ţări studiază aceste riscuri potenţiale.

În ceea ce priveşte efectele utilizării operaţiilor informaţionale, prima observaţie este costul relativ scăzut al unui atac asupra sistemelor informaţionale şi comunicaţiilor în reţea. Acesta este trivial în comparaţie cu mijloacele militare convenţionale. O combinaţie de computere şi minţi pregătite şi pline de imaginaţie este suficientă pentru a produce efecte operaţionale majore (evident, la nivelul entităţilor care depind major de infrastructură).

Conştient sau nu, la toate nivelurile, se acţionează în prezent pentru întărirea interoperabilităţii şi reducerea măsurilor de protecţie în beneficiul vitezei. Toate aceste

78 John Arquilla şi David Ronfeldt, In Athena 's Camp, Preparing for Conflict in the Information Age, http://www.rand.org./publications/MR/ MR880/contents.html

mecanisme, într-un fel sau altul, favorizează creşterea vulnerabilităţilor şi a intruziunilor, în contextul în care factorul timp în planul contramăsurilor, tinde spre zero (dacă un atac convenţional cere timp pentru organizarea, pregătirea şi dispunerea forţelor, un atac informaţional poate să înceapă la puţin timp după decizia de a se desfăşura).

Operaţiile informaţionale sunt un mod de gândire şi... o invitaţie la reflecţie. Este momentul unei schimbări de paradigmă!

SIGURANŢA INFORMAŢIONALĂ EXPERIENŢA CANADIANĂ

TITT T. ROMET*

Această lucrare va descrie iniţial elementele unui larg cadru conceptual care a fost utilizat. El va descrie apoi conceptul specific dezvoltat în cadrul CF (Forţelor Canadiene) şi o evidenţiere a structurilor ce au fost formate. Lucrarea trece în revistă lecţiile învăţate, cele ce sunt în curs de învăţare şi cele ce urmează să fie învăţate precum şi dificultăţile avute în abordarea holistică privind dezvoltarea unui program de operaţii informaţionale, atât la nivel militar cât şi la nivel guvernamental.

Cu cinci ani în urma, Forţele Canadiene (CF) s-au confruntat cu decizia de a integra operaţiile bazate pe informaţii în activitatea militară curentă. Cu evoluţia rapidă a tehnologiilor de comunicaţie şi tehnologiilor calculator, informaţia a fost recunoscută ca o resursă strategică ce trebuie administrată efectiv.

Canada era deja integrată sub aspectul reţelelor cu SUA în numeroase domenii înrudite cum ar fi telecomunicaţiile şi sistemul bancar. Confruntată cu creşterea globală a schimburilor comerciale şi de informaţie prin intermediul extinderii reţelelor de comunicaţii, a fost necesar să se înţeleagă faptul că imaginea tradiţională a graniţelor nu mai există.

Aşteptările nu au fost create numai în sectorul militar ci şi în cel guvernamental şi privat unde informaţia poate fi obţinută instantaneu, analizată şi schimbată. Internetul a

devenit reţeaua prin care informaţiile personale (private), informaţiile de afaceri

Consultant privat şi cercetător, anterior cercetător ştiinţific al apărării. Canada şi chiar informaţii militare (senzitive) ar putea fi schimbate. Atât eficienţa noastră economică cât şi militară a fost sporită pe baza sistemelor informaţionale automate şi a reţelelor.

Mai mult, pentru reducerea costurilor şi crearea de noi elemente de eficienţă, militarii au integrat tot mai mult tehnologii militare în sistemele lor militare. Noi descriem aceste fenomene ca fiind „transformarea civilă a militarilor'4.

Cu militarii SUA mişcându-se foarte rapid în acest nou domeniu, pe care ei l-au numit iniţial „Război informaţional", Canada a avut nevoie să abordeze principalele probleme cu carc se confruntă. CF a înţeles că nu are resursele umane şi financiare pentru a urma abordarea SUA şi că are nevoie să dezvolte un cadru conceptual în conţinutul căruia principalele cerinţe să poată fi analizate şi implementate.

Este general acceptat că apariţia activităţii bazate pe informaţii este legată direct de progresele tehnologice care au avut loc pe parcursul ultimelor decade şi ale aplicaţiilor lor. Domeniile tehnologice cheie, care se află în spate, sunt comunicaţiile, senzorii şi calculatoarele.

Extinderea şi varietatea comunicaţiilor care au fost vast dezvoltate îmbunătăţesc opţiunile, complexitatea şi caracterul critic al informaţiilor pe care le vehiculează. Prin mijloacele de transmisie care oferă alegeri mai multe, ce variază de la fără fir, cabluri de cupru în bandă largă, la fibre optice, disponibilitatea progresiv crescătoare a numărului de canale, a lărgimilor de bandă şi a tipurilor de circuite (ex. prin satelit, cablu TV) s-a extins domeniul şi s-a scurtat timpul în care informaţia poate fi schimbată.

Informaţia este acum disponibilă printr-un mare număr de surse, şi în special din perspectiva militară, de la senzori ne-umani. Întreg spectrul electromagnetic poate fi exploatat pasiv sau activ prin mijloace de culegere diferite

cum ar fi radio, radar, infraroşu / electrono-optic şi radar cu aparatură sintetică. În paralel, contra măsurile au evoluat de asemenea la o mascare mai bună, inducerca în eroare sau ascunderea obiectelor de interes.

Evoluţia constantă a componentei hardware şi software a calculatorului prin creşterea dimensiunii, puterii şi aplicabilităţii odată cu reducerea în dimensiune şi cost, reprezintă o reamintire zilnică a dificultăţii de a sta în domeniul de vârf al tehnologiei informaţiei.

Nu a evoluat numai baza tehnologică pentru societatea bazată pe informaţie ci şi sistemele şi organizaţiile care utilizează tehnologie au crescut în număr şi complexitate. Suportul de ştiri acoperă în prezent activitatea globală pentru 24 de ore, 7 zile pe săptămână fiind în creştere, şi este disponibil în mod egal pentru un număr mai mare de populaţie din întreaga lume.

Reţeaua Internet a devenit substratul de conduită pentru o mare parte a schimbului de informaţii şi comunicaţii. Ea a evoluat dramatic de la începuturile ei, o propunere a corporaţiei RAND ca reţea de supravieţuire nucleară utilizând elemente individuale nesigure sau elemente vulnerabile aşa încât capabilitatea şi funcţionalitatea sistemului să poată să se manifeste. Astăzi, cererea de informaţii prin intermediul Internet se suprapune cu preocupările pentru securitatea şi integritatea informaţiei, sau credibilitatea sursei. Consecvent, chiar astăzi, informaţia poate fi expusă interceptării, distorsionării sau furtului.

Comerţul electronic este domeniul economic care a crescut cel mai rapid. Legal sub formă de bani, stocuri, bunuri şi multe alte tranzacţii se realizează acum electronic sau sunt numai o intrare electronică într-o bancă de date. Comerţul Canadei, (şi astfel cel al CF), este în mare măsură dependent de intimitatea şi precizia Internetului şi a echivalenţilor lui comerciali.

În timp ce SUA a început explorarea şi activitatea ei pentru Operaţii Informaţionale din domeniul militar, Canada a ales ca punct de start mediul informaţional

global (OIE). GIE a fost definit de indivizi, organizaţii sau sisteme în afara sferei de control militar, însă cuprinde mediul informaţional militar (MIE) definit separat şi distinct.

S-a considerat că toate „operaţiile” au loc în GIE şi din cauza progreselor tehnologice, operaţiile militare pot fi vizualizate, analizate şi diseminate audienţei globale în timp aproape real. De fapt poate fi arătat că informaţia ar putea fi distribuită mai repede prin intermediul legăturilor comerciale decât prin mijloace guvernamentale sau militare.

Pentru a sprijini GIE, există infrastructura de informaţie globală (GII) care este o interconectare a reţelelor de comunicaţii, calculatoare, baze de date şi consumatori electronici ce permit accesul la informaţie a unei audienţe largi. Ea este legată global şi este caracterizată de unirea reţelelor şi tehnologiilor informaţionale militare şi civile.

Există în cadrul GII, infrastructura informaţională naţională (NII), care constă într-o serie de componente ce includ reţelele informaţionale publice (guvernamentale) şi private sprijinând preocupările, activităţile şi organizaţiile naţionale. Nu există graniţe discrete între GII şi NII; de fapt, accesul global la informaţie devine tot mai critic pe măsura globalizării pieţelor, resurselor şi economiilor. Infrastructura informaţională a apărării (DII) este inclusă în cadrul infrastructurilor menţionate mai sus, oferind suport pentru misiuni, comandă şi control şi reţele de intelligence pentru militari.

În cadrul conceptual a fost stabilită o structură care ar putea să se adreseze preocupărilor de intimitate, confidenţialitate şi procesului de luare al deciziei. Deoarece au fost dezvoltate multe modele diferite şi sisteme pentru a descrie luarea deciziei ele au aceleaşi elemente de bază comune:

a. achiziţia datelor;

b. prelucrarea şirurilor de date în informaţii utile care vor conduce la înţelegere;

c. compararea cu starea existentă sau curentă;

d. decizia de implementare, direcţionare etc.

Este important de înţeles că în cadrul ciclului de luare a deciziei există două entităţi distincte aflate în legătură care contribuie în final la luarea deciziei. Există un *domeniu informaţional* care este compus din trei elemente:

a. un set specificat de bunuri informaţionale;

b. utilizări autorizate ale informaţiei;

c. O politică de securitate ce guvernează utilizarea bunurilor informaţionale.

Ca un exemplu, bunurile informaţionale ar putea să includă toate înregistrările medicale şi informaţia despre un individ în cadrul unui plan de sănătate elaborat la nivel guvernamental. Politica de securitate ar trebui să specifice cum este informaţia protejată, cine are acces, cum este informaţia stocată, prelucrată, etc.

Cealaltă entitate este *sistemul informaţional* actual, care cuprinde componentele de prelucrare şi comunicare ce trebuie să încorporeze elementele şi politicile de securitate scoase în evidenţă în domeniul informaţional.

Structura actuală a sistemului informaţional poate fi separată în trei straturi care se suprapun unul peste altul şi sunt bazate pe funcţia lor: fizică, logică şi semantică. Această împărţire pe categorii a fost folositoare în înţelegerea vulnerabilităţilor informaţiei în cadrul oricărei structuri informaţionale. La bază se află stratul fizic care poate fi descris de elementele hardware ale sistemului informaţional.

Aceasta ar putea include clădiri, calculatoare, echipamente de comunicaţie şi chiar personal. Această imagine conduce natural la conceptul de realizare a analizei „legături şi noduri”. Stratul din mijloc este stratul logic care constă în modul cum structura este operată, pachetele soft, sistemele, prelucrarea datelor în i informaţii şi în final în cunoştinţe, distribuirea informaţiilor şi [procedurilor de operare. Al treilea şi cel mai înalt nivel se numeşte nivelul semantic şi reprezintă conţinutul şi

interpretarea informaţiei incluse în cadrul sistemului informaţional.

Nivelul fizic este vulnerabil la distrugerea fizică şi este obiectul sistemelor de arme militare tradiţionale. Deoarece infrastructurile militare şi civile devin tot mai integrate, un mai mare accent trebuie să fie pus pe analiza nodurilor şi legăturilor pentru a asigura ţintirea cu eficacitate. Scopul afectării nivelului logic este de a interfera cu funcţiile sistem.

Atacurile ar putea include întârzierea executării de proceduri, direcţionarea greşită a informaţiei sau infectarea cu viruşi software, în cazul afectării ideale, atacatorul nu-i nevoie să distrugă informaţia sau sistemul ci doar să le controleze. La nivelul cel mai înalt, nivelul semantic, obiectivul atacului este afectarea şi/ sau exploatarea încrederii pe care utilizatorul o are în sistemul informaţional, în reţea, şi în abilitatea lui de a interpreta şi a lua decizii pe baza informaţiei. Cadrul nostru larg accentuează faptul că ceea ce militarii numesc Operaţii Psihologice trebuie să aibă un context mult mai larg în descrierea infrastructurilor informaţionale globale sau naţionale.

Cadrul larg ce a fost prezentat a încercat să arate cum capacitatea societăţii de a face faţă războiului depinde de fiecarc componentă a infrastructurii tehnologice care există în prezent. Creşterea continuă a interdependenţelor dintre infrastructurile civile şi militare, necesită schimbări ale modului în care conflictul este tratat, lansează provocări pentru proiectarea instituţiilor tradiţionale şi a ierarhiilor şi redesenează conceptul de graniţe şi securitate naţională. Aşa cum a spus Tedlers, societăţile poartă război prin mijloacele lor de a produce bogăţie şi noi suntem, sau ne deplasăm spre era informaţională.

Bazat pe dezvoltarea conceptului iniţial, şi apoi prin vizite, întâlniri şi discuţii, Forţele Canadiene au formulat viziunea lor despre Operaţiile informaţionale (IO). Pentru CF, IO merg dincolo de sistemele informaţionale simple şi

procese, şi chiar IO ar trebui văzute că o STRATEGIE, NU ca pe o capabilitate însăşi.

Dacă este văzută ca o strategie, atunci obiectivul IO devine factorul de decizie, fie că este preşedinte, prim ministru, comandant sau membru de serviciu individual, marinar, soldai sau aviator. Totuşi, IO devine o strategie ce integrează diferite capabilităţi de realizare a obiectivelor politice şi militare. Urmează apoi că IO include un doneniu larg de capabilităţi ce ar putea să cuprindă activităţi militare – tradiţionale cum ar fi distrugerea, inducerea în eroare, OPSEC, EW, PSYOPS (C2W) pentru activităţi bazate pe tehnologie cum ar fi atacuri la reţeaua de calculator, sau afaceri civile, afaceri publice şi chiar afaceri legale.

Pentru CF, definiţia devine: *„Acţiuni desfaşurate în sprijinul obiectivelor politice şi militare care influenţează factorul de decizie prin afectarea informaţiei şi/sau a sistemelor informaţionale ale celuilalt simultan cu exploatarea şi protejarea propriilor informaţii şi/sau sisteme informaţionale*”

Definiţia CF pentru IO arăta că informaţia reprezintă un mijloc şi factorul de decizie reprezintă finalitatea. Definiţia minimizează intenţionat importanţa aspectelor tehnice ale IO şi se concentrează pe toate măsurile ce ar putea fi utilizate pentru a influenţa factorul de decizie.

În timp ce multe dezbateri au avut loc în Canada, precum şi în lume pentru definirea IO, definiţia CF a vrut să fie de ansamblu (largă). Astfel, ea poate fi aplicată activităţilor naţionale, internaţionale, civile sau militare şi se aplică la fel pentru situaţii de pace, criză sau război.

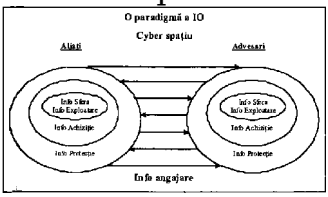


Figura 1: Paradigma operaţiilor informaţionale (IO).

Paradigma IO care a fost dezvoltată pentru a

prezenta mesajul CF şi ceea ce a devenit baza pentru dezvoltarea structurii CF au fost o serie de „sfere” de informaţii aşa cum se arăta în figura de mai sus.

Mediul, care a fost numit din lipsa de alte cuvinte mai bune cyber spaţiu, conţine ansamblul tuturor informaţiilor, atât ale adversarilor cât şi ale prietenilor. Există patru procese de bază care pot fi realizate în cyber-spaţiu: exploatarea informaţiei, achiziţia, protecţia şi intrarea în conflict cu înţelegerea că aceleaşi activităţi pot fi desfăşurate simultan de oricare adversar.

CF doreşte să fie în măsură să exploateze informaţia de care dispune. Aceasta implică existenţa unui sistem desemnat să furnizeze informaţia corespunzătoare utilizatorului corespunzător la momentul potrivit. CF va avea nevoie să achiziţioneze informaţia, cea despre adversarii noştri posibili din diferite surse de intelligence şi prin alte mijloace cât şi despre aliaţi şi prieteni pentru a asigura compatibilitatea. Oricând se culege sau se exploatează informaţie, este nevoie de a proteja informaţia şi procesele prin care se culege şi se exploatează. Acest proces va include atât protecţia faţă de adversarii noştri, prin detectarca pătrunderii în sistem/calculator şi reacţia corespunzătoare faţă de noi înşine, cum ar fi angajaţii nemulţumiţi sau viruşii.

Aspectul de protecţie include de asemenea posibilitatea de a recupera şi de a utiliza echipamentele după pătrunderea neautorizată sau disfuncţionalităţi. În final, CF are nevoie să facă faţă adversarilor (sau „inamicilor”) prin încercarea de a preveni sau limita posibilitatea lor de a achiziţiona informaţii, realizată prin mecanisme de protecţie şi obţinerea sau deţinereâ controlului informaţiilor lor şi/sau proceselor.

Rezultă din aceste patru procese şi funcţii, exploatarea, achiziţionarea, protejarea şi intrarea în conflict, că CF are dezvoltate structura şi activităţile Grupului său de IO pentru a li în măsură să-şi îndeplinească responsabilităţile şi mandatele.

Paralel cu acest efort, Departamentul Apărării, a

implicat de asemenea alte departamente guvernamentale şi Biroul Consiliului

Privat (activităţi guvernamentale centrale) atât la nivel executiv cât şi de conducere, pentru a stabili un răspuns guvernamental coordonat la ameninţări şi vulnerabilităţi. DND a înţeles că are un rol important dejucat ca partener în procesul mai larg desfăşurat de Guvernul Canadei. Această viziune s-a integrat bine cu conceptul mai larg al Infrastructurilor Informaţionale Globale şi Naţionale, protecţia lor şi rolul Canadei în cadrul acestor procese.

Iniţial CF a stabilit un grup de lucru pentru IO pentru a aborda multe din problemele care erau nevoie să fie investigate pentru ca militarii să devină valoroşi în domeniul IO, incluzând conceptele, doctrinele, politicile, cerinţele CF şi instruirea. Gupul a cuprins componentele majore ale DND (Departamentul Apărării Naţionale), incluzând Operaţii J3, servicii de informaţii, structuri de servicii, aspecte legale, politici, ofiţeri de securitatea informaţiei (CIO) şi domeniul afacerilor publice.

Încă de la început, CF a restructurat grupul pentru a forma Grupul de Operaţii Informaţionale al CF (CFIOG). Acest efort a integrat şi consolidat multe funcţii ce se legau de activităţile de IO pentru a forma o singură voce care să reprezinte activităţile de IO. Au fost stabilite noi activităţi bazate pe paradigma de IO ce a fost descrisă mai devreme.

O Echipă de Evaluare a Vulnerabilităţilor Naţionale (NVAT) a fost stabilită iniţial pentru a începe rolul de protecţie a resurselor de informaţii a CF. Această activitate a fost acum preluată de Echipa de Răspuns la Incidente Calculator (CIRT) şi care stabileşte în prezent mecanismele pentru detectarea, raportarea şi investigarea încercărilor de pătrundere neautorizată în sistemele informaţionale ale militarilor.

În paralel cu aceste eforturi, a fost scrisă, aprobată şi diseminată doctrina CF. Doctrinele individuale ale serviciilor au fost pregătite şi integrate cu cadrul mai larg

al Doctrinei CF. Pe frlăsură ce aceste aspecte au fost completate fără întârzieri majore, dezvoltarea Politicii CF a fost mult mai dificilă. Cele mai ample probleme au generat preocupări privind rolul şi activitatea PSYOPS, legătura acesteia cu Afacerile Publice, şi aspecte legale ale activităţilor IO ofensive şi defensive. Unele dintre elementele cheie ale conţinutului politicii recent aprobate sunt:

a. IO reprezintă o strategie integrată ce se concentrează pe toate aspectele de influenţare a factorilor de decizie.

b. IO nu reprezintă o simplă problemă tehnică, dar include lucruri cum ar fi afacerile (activităţile) publice, PSYOPS şi vulnerabilităţi ale infrastructurii guvernamentale.

c. Comandanţii sunt responsabili pentru implementarea IO defensive.

d. Coordonarea IO va fi realizată de către o Celulă de Coordonare a Operaţiilor informaţionale (IOCC).

Conceptul de IOCC a fost desemnat pentru a furniza intrări de IO pentru planurile dezvoltate de către Statul Major Naţional. Structura s-a dorit să fie flexibilă, adaptată pentru a îndeplini cerinţele specifice. Pe măsură ce conceptul a fost acceptat, el trebuie încă să fie activat consistent în cadrul exerciţiilor şi operaţiilor. Introducerea IO necesită regândirea profundă de către statul major şi realinierea preocupărilor pentru toate procesele de planificare. Va fi, fără îndoială, nevoie timp pentru ca aceste consideraţii să devină un element uzual pentru planificatorii de IO.

De la primele stadii ale dezvoltării conceptului de IO, s-a afirmat clar că este nevoie că reprezentanţii comunităţii de R&l) să fie implicaţi în sprijinirea procesului de IO specific CF. Fiecare dintre procesele de IO definite în paradigma de IO: protecţia, exploatarea, achiziţia şi tratarea adversarului necesită o contribuţie importantă a R&D pentru ca CF să-şi îndeplinească rolul pe deplin Acest rol a devenit o provocare particulară în

cadrul legăturii realizate între tehnologiile şi cerinţele militare şi civile.

În cadrul CF, J6 a primit rolul de coordonare a dezvoltării IO. Un stat major restrâns de IO formează nucleul permanent eu rol de coordonare a IO şi furnizează vizibilitatea necesară K > pentru a implementa schimbări. Acest rol nu include numai funcţiile CF şi ale Guvernului Canadei, ci şi legăturile noastre internaţionale. Ei au avantajul de a realiza implementarea conceptelor de IO şi de a stabili structurile care să corespundă cerinţelor.

Conceptul de bază ce a fost stabilit iniţial şi menţinut pe parcursul procesului de dezvoltare al IO a fost că IO reprezintă o strategie care cuprinde un mediu informaţional care depăşeşte pe cel specific numai domeniului militar. Această abordare holistică necesită totuşi contribuţii din partea tuturor pentru a funcţiona efectiv, altfel DND operează în vid.

Cea mai mare dificultate înregistrată de DND este probabil reluctanţa (nedorinţa) Guvernului Canadei de a accepta rolul conducător care este necesar în abordarea holistică şi un rol în care toţi participanţii implicaţi să-l considere ca necesar. Apărarea naţională se vede ea însăşi ca un element important, dar reprezintă numai un membru cooperativ integrat într-un rol naţional mai larg.

Altă dificultate ce a apărut în situaţia Canadei a fost încrederea în încorporarea de dezvoltări de IO şi studii ce-şi au originea în afara poziţiei Canadei. Aceasta va diminua rolul Canadei ca un inovator de IO, atât în domeniul militar cât şi civil. Totuşi, se poate afirma că prin adoptarea unei abordări prudente, Canada va evita greşelile repetate de dinainte, dar la un cost de pierdere a unicităţii ei, care ar putea fi stabilit. Totuşi, în acest proces, DND este gata să meargă mai departe pe arena IO fără avantajul unei conduceri centrale puternice.

Nu este totuşi surprinzător, că rămâne numai Canada una dintre ţările vestice/ avansate tehnologic a cărui guvern nu a sponsorizat existenţa unei echipe de răspuns la incidentele calculator. În cadrul abordării holistice

adoptate de DND, conceptul de informaţie ca bun naţional reprezintă o premisă fundamentală şi ca rezultat necesită să fie luate în considerare măsuri de securitate naţională corespunzătoare.

În mod sigur un avantaj al abordării holistice a fost dezvoltarea reilativ uniformă a politicii şi doctrinei DND. În particular, integrarea politicilor şi doctrinelor individuale ale serviciilor a fost făcută mai uşor. Încercarea de a realiza un consens departamental, lăsând deoparte consensul naţional, este mult mai dificilă dacă aceasta este condusă de jos în sus.

Introducerea IO în Departament a creat oportunitatea pentru stabilirea de noi roluri, în special în unele locuri tradiţionale. De exemplu, pentru J6 care era tradiţional responsabilă pentru sprijin de comunicaţii şi sprijin electronic s-a găsit ea însăşi în măsură să controleze „arme operaţionale" în forma calculatoarelor şi reţelelor. În timp ce J6 în Canada a crezut ferm în rolul său de conducere a elementelor operaţionale ale departamentului ce revin domeniului IO, lor au trebuit să le fie date responsabilităţi în domenii ce nu erau tradiţional în mandatul lor.

Deoarece tranziţia înceată înspre Grupul de IO a avut loc, a fost evident că un număr de roluri şi structuri tradiţionale urmau să fie schimbate. A fost o caracteristică a multor organizaţii, nu numai a DND dar peste tot la fel, a existat tendinţa de a consolida şi proteja structurile şi funcţiile existente. Chiar cu o abordare holistică pentru IO, şi în dezvoltarea organizaţională în general, mai curând decât să se opereze intern şi protectiv, este mai benefic să se îmbunătăţească competenţele şi funcţiile. Aceasta este o lecţie dificil de învăţat.

Cu noul concept IO, este de asemenea necesar să fie pregătii personal cu un nou set de capabilităţi şi să fie plasat în roluri noi, netradiţionale. Înseamnă că trebuie create noi oportunităţi de instruire, şi în cadrul sistemului de personal, recunoaşterea roluri lor noi şi a responsabilităţilor ce sunt asociate cu îndeplinirea

funcţiilor legate de IO.

Abordarea holistică a făcut aceste oportunităţi să se dezvolte mai încet decât rolurile tradiţionale, şi instruirea primeşte încă cea mai mare atenţie şi sprijin. Personalul militar nu mai poate să aştepte să fie numit într-o nouă poziţie pentru trei ani şi apoi să se mute. Instruirea şi cerinţele pentru lucrul în cadrul IO necesită <> implicare mai lungă şi o instruire permanentă, pentru a rămâne în top. Aceste probleme necesită încă rafinare în cadrul CF pentru a beneficia din plin de programul de IO.

Comunitatea militară de R&D s-a aflat într-o poziţie dificilă, în primul rând ea trebuia să se lupte cu resursele guvernamentale reduse. În al doilea rând, şi mai important, ea trebuia să facă faţă competitorilor civili/comerciali ce se aflau în topul tehnologic de un număr de ani.

Aceasta însemna de asemenea că rolul tradiţional al R&D trebuia să se schimbe sau să se adapteze la a fi un integrator de top mai curând decât a fi un inovator. Aceasta este relevant în special în situaţia Canadei care produce adesea sisteme complete dar mai frecvent furnizează componente sau produce sisteme hibride ce integrează tehnologii şi concepte numeroase. La fel pentru a menţine pacea cu sectoarele civile şi comerciale, conceptele anterioare de cercetare pe termen lung, mediu şi scurt au trebuit să fie regândite.

Din cauza creşterii integrării necesare, este aproape o necesitate pentru oamenii de ştiinţă R&D să lucreze mână în mână cu operatorul pentru a fi integrat deplin în strategia operaţională de IO.

De la grupurile de lucru iniţiale de IO, a fost mai mult decât clar că noi alocări financiare ar putea fi aşteptate pentru activitaţi de IO. S-a aşteptat ca fondurile existente să fie re-alocate pentru a face faţă nevoilor. Într-o abordare holistică, oportunităţile de a găsi fondurile realocate sunt dificile, deoarece fiecare organizaţie şi fiecare manager va încerca să-şi protejeze resursele limitate.

Chiar abordarea SUA de a lucra cu elementele

serviciilor individuale duce eventual la un punct unde nu există pe mai departe oportunitatea de a realoca sau ajusta fonduri. Deoarece IO a fost introdus ca un nou concept cu propriul său set de ameninţări şi vulnerabilităţi, a devenit necesară injectarea de noi fonduri şi personal în acest domeniu.

războiul informaţional probleme de securitate

Dr. W. STEIN4

Scopul acestei lucrări este de a găsi orientările, ilustraţiile utile, precum şi definiţiile, şi poate factorii critici care pot ajuta la deschiderea unei porţi pentru cooperarea mai bună în domeniul cercetării, dezvoltării şi educaţiei corespunzătoare problemelor prezente legate de securitatea informaţiei. Acest domeniu include Securitatea Informaţiei (INFOSEC),

Războiul informaţional (IW) şi Protecţia Infrastructurii Critice (CIP). Se pot găsi mulţi factori tradiţionali ce influenţează înţelegerea şi cooperarea ce pot să includă termeni şi definiţii diferite, competiţia economică, şi interese de securitate naţională. Rezultă că există un domeniu de probleme comune în contextul războiului informaţional, cu provocări pentru un nou nivel de cooperare în ştiinţă, inginerie şi educaţie.

A fost acceptat în timp că sectorul de informaţii şi comunicat i i cu sistemele şi infrastructurile lor informaţionale reprezintă un element central al tuturor celelalte sectoare ale societăţilor moderne, necesare pentru funcţionarea de bază a fiecărui aspect naţional şi internaţional. Atacurile asupra sistemelor informaţionale reprezintă deja un fapt cotidian al erei informaţionale.

Aproape zilnic, hackerii exploatează vulnerabilităţile din infrastructura noastră informaţională globală şi din sistemele de calcul. Diferiţi adversari ideologici şi culturali – individual, grupuri de guerrilă şi grupuri teroriste – sunt pe cale să descopere „Războiul

* Armata Germană.

informaţional” ca un mijloc major de afectare a activităţilor din sectorul guvernamental, militar şi cel al

corporaţiilor. Guvernele, forţele armate şi societatea ca un întreg, au nevoie de a fi pregătiţi în scopul de a face faţă acestor ameninţări şi atacuri informaţionale. Dar în mod curent se pare că există o lipsă de conştientizare privind securitatea informaţională şi vulnerabilităţile infrastructurilor.

Deşi o categorie redusă din aceste atacuri se concretizează în pierderi sau pagube semnificative, marea lor majoritate se (concretizează în pagube mici sau inexistente, echivalentul infracţional al pătrunderii neautorizate, deranjarea liniştii publice, ' vandalism minor, şi chiar furt.

, A fost estimat că mai mult de 90% din aceste atacuri se [desfăşoară utilizând unelte şi tehnici disponibile (pe baza i incidentelor raportate de CERT), că numai un atac din 20 este ' conştientizat de către o victimă, şi numai 1 atac din 20 este raportat (aceste ultime două statistici sunt un rezultat al studiului desfăşurat;de Agenţia Sistemelor Informaţionale ale Apărării) şi rate similare au fost raportate de către alţii). Totuşi, se pare că ratele de raportare sunt în creştere. Şi aşa cum se poate vedea, nu există (aproape) jnimic nou în acest domeniu.

Ca o consecinţă, interesul pentru securitatea informaţiilor, calculatoarelor şi reţelelor a apărut devreme şi primul raport datează din 1970. După apariţia programului de Protecţie a Infrastructurii Critice (CIP) pe parcursul ultimilor 5-10 ani, noi ne confruntăm acum cu trei domenii referitoare la securitate cu provocări aflate în legătură: Securitatea Informaţiei (INFOSEC),

Războiul Informaţional (IW) şi Protecţia Infrastructurii Critice (CIP). Când analizăm problemele referitoare la securitate, putem să găsim diferiţi termeni, uneori definiţii redundante şi domenii care se suprapun (diferit între comunităţi, naţiuni, etc.), de exemplu securitate, siguranţă, şi protecţia şi/sau infrastructurilor precum şi război informaţional şi operaţii informaţionale.

Aceste componente eterogene şi diverse pot face cooperarea dificilă sau chiar imposibilă. Figura 1

evidenţiază domeniile de

Război Informaţional (IW), Securitatea Informaţiei (INFOSEC), şi Protecţia Infrastructurii Critice (CIP) precum şi posibilele lor subdomenii aflate în legătură. Deşi cele trei domenii au multe subiecte comune (ex., metode, instrumente, în parte utilizând aceleaşi infrastructuri, având obiective de cercetare şi dezvoltare similare, utilizând cadre de lucru pentru analiză similare), gradul de cooperare în cercetare şi dezvoltare pare să fie foarte limitai.

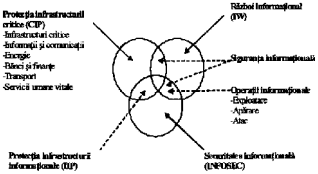


Figura 1. Domenii şi subdomenii ale războiului informaţional, securităţii informaţionale şi protecţiei infrastructurii critice

Termenul de „securitate informaţională” (INFOSEC) este în uz de aproape două sau trei decenii. Standardul federal al SUA îl defineşte ca *„Protecţia informaţiei împotriva dezvăluirii, transferului, modificării, sau sustragerii neautorizate făcută accidental sau intenţionat*. „ Prin contrast, termenul de „siguranţă informaţională” este relativ nou. În 1996 directiva Departamentului Apărării SUA îl defineşte ca *„Operaţii informaţionale ce protejează şi apără informaţiile şi sistemele informaţionale prin asigurarea disponibilităţii, integrităţii, autenticităţii, conßden ţialităţii şi non-repudierii lor. Aceasta include suport pentru restaurarea sistemelor informaţionale prin încorporară capabilităţilor de protecţie, detecţie, şi capabilităţi de reacţie*. „ Războiul informaţional defensiv este legat îndeaproape de ambele concepte, dar se preocupă numai de atacurile intenţionate. Securitatea informaţională şi siguranţa informaţională abordează de asemenea ameninţări neintenţionate, ex. erori, accidente, şi dezastre naturale.

Astfel, siguranţa informaţională este bazată pe definiţia operaţiilor informaţionale şi are un înţeles oarecum mai larg decât securitatea informaţională. Termenul de siguranţă informaţională poate fi întâlnit în diferite domenii guvernamentale, ex. Departamentul Apărării,

Protecţia Infrastructurilor Critice şi Agenţia de Securitate Naţională. NATO defineşte operaţiile informaţionale ca *99Acţiuni desfaşurate pentru a influenţa factorii de decizie în sprijinul îndeplinirii obiectivelor militare şi politice, prin afectarea informaţiilor altora, proceselor bazate pe informaţii, sisteme de comandă şi controlsimultan cu exploatarea şi protejarea propriei informaţii şi/sau sistemelor informaţionale*".

Există două categorii principale ale Info Ops: Info Ops defensive şi Info Ops ofensive, depinzând de natura acţiunilor implicate.

Aşa cum indică figura 2, provocarea curentă este pentru securizarea sistemelor informaţionale conectate în reţea atât din mediul militar cât şi civil. Consecvent Organizaţia de Securitate a Sistemelor Informaţionale din cadrul NSA a definit un sistem informaţional (IS) ca:

„întreaga infrastructură, organizare, personal şi componente pentru culegerea, prelucrarea, stocarea, transmiterea, afişarea, diseminarea şi eliberarea de informaţii"*şi* securitatea sistemelor informaţionale (ISS) ca: *protecţia sistemelor informaţionale împotriva accesului neautorizat sau modificării informaţiei în etapa stocării, prelucrării sau tranzitului, şi împotriva interzicerii serviciului pentru utilizatorii autorizaţi, incluzând acele măsuri necesare pentru detectarea, documentarea şi contorizarea a astfel de ameninţări*".

Securizarea sistemelor informaţionale conectate în reţea necesită o perspectivă acoperitoare asupra sistemului. Securitatea este îndeaproape legată de siguranţă şi încredere şi nu trebuie ignorată sau atribuită preocupărilor incidentale. Noi abordăm aici o vedere mai largă a problemelor ce ţin de securitate şi siguranţă, şi

considerăm aceste probleme ca o problemă globală unificată la nivelul sistemului/ reţelei/ agenţiei.

Procedura de securizare indicată în figura 2, poate fi aplicată unui singur calculator, precum şi sistemelor şi infrastructurilor de IT la nivel naţional.

Vulnerabilităţile sistemelor (figura 2) sunt omniprezente. Cele mai multe sisteme de operare au un sistem de autentificare slab şi sunt uşor de penetrat. Cele mai multe din aceste sisteme au elemente de control al accesului slabe şi tind să fie configurate defectuos şi ca rezultat există cu uşurinţă posibilitatea utilizării greşite odată ce este obţinut accesul iniţial.

Aceste sisteme au adesea facilităţi de monitorizare care sunt adaptate greşit, pentru a determina când au loc ameninţările şi ce pericole pot să apără. Uneori, utilizarea greşită de către cei din afară şi din interior este posibil să se realizeze şi uneori foarte dificil de detectat.

Ameninţările la securitate (figura 2) sunt omniprezente. Domeniul ameninţărilor ce pot exploata aceste vulnerabilităţi este enorm, plecând de la activităţi teroriste posibile, sabotaj, spionaj, competiţie industrială sau naţională, reproducere neautorizată, funcţionări mecanice defectuoase şi erori umane.

Atacurile pot implica inserări de Cai Troieni, sau intervenţii fizice, incluzând acţiuni plătite de angajaţi nemulţumiţi sau acţiuni de persecuţie. Atacurile de interzicere a serviciului sunt insidioase în particular, deoarece este dificil de a realiza apărarea împotriva lor şi efectele lor pot fi devastatoare. Sistemele conectate la Internet sau disponibile prin linii de conexiune sunt victime posibile ale pătrunderilor externe.

Chiar sistemele ce par să fie complet izolate sunt subiect de

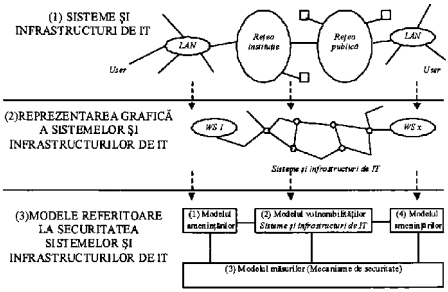


Figura 2. Paşi în securizarea sistemelor informaţionale: *analiza vulnerabilităţilor*, *ameninţărlor şi riscurilor* utilizare internă greşită. Suplimentar, multe din aceste sisteme ce par izolate pot fi compromise prin acţiune de la distanţă din cauza facilităţilor lor de diagnosticare şi mentenanţă de la distanţă.

Riscurile sunt omniprezente (figura 2). Consecinţele acestor vulnerabilităţi şi a ameninţărilor asociate denotă că riscurile pol fi considerabile. Utilizarea greşită a calculatoarelor poate avea ca rezultat (de exemplu pierderea de confidenţialitate: pierderea integrităţii sistemului atunci când sistemele sunt afectate, pierderea integrităţii datelor atunci când datele sunt alterate, interzicerea serviciului ce fac resursele furnizate nedisponibile, sau chiar furturi de servicii).

Securitatea informaţională (INFOSEC) este fundamentală şi sub unele aspecte reprezintă chiar o parte clasică a celor trei probleme referitoare la securitate. Securitatea informaţională (sau securitatea calculatoarelor, cum a fost ea numită iniţial), a fost pentru prima dată prezentată într-o formă completă într-un raport din anul 1970 al Biroului de Ştiinţă al Apărării, dar experienţa practică şi operaţională, în particular încorporarea măsurilor de securitate în cadrul sistemelor, a avut loc mult mai târziu.

Securitatea calculatoarei or ca disciplină a fost studiată pentru prima dată la începutul anilor 1970 deşi problemele referitoare la aceasta au influenţat dezvoltarea anterioară a multor sisteme. Deceniul anilor 1970 a fost

caracterizat de cercetările finanţate de Departamentul Apărării, în special de către Forţele Aeriene şi DARPA. Experienţa celorlalte naţiuni (lumii întregi) nu s-a manifestat până la publicarea lucrării „Criterii de evaluare a încrederii în sistemele de calcul specifice Departamentului Apărării”, cunoscută sub denumirea de „Cartea Portocalie” sau TCSEC.

De-a lungul anilor 1970 şi 1980, eforturile INFOSEC s-au concentrat pe criterii de evaluare a încrederii în securitatea calculatoarelor neconectate în reţea (TCSEC) şi securitatea comunicaţiilor (COMSEC) pentru comunicaţii militare şi naţionale. Chiar şi aşa, sisteme care încorporează măsuri de securitate nu au fost instalate până în ultima parte a anilor 1980.

Subiectul operaţiilor informaţionale a fost dezvoltat în experimente de către forţele SUA, în special între anii 1985-1995. Începând cu ultima parte a anilor 1980 a existat un interes sporit în protejarea infrastructurilor critice de care societatea depinde pentru a face faţă atacurilor fizice şi informaţionale. Institutul Tehnologiilor Critice (condus de RAND) a fost creat în 1991 pe baza unei hotărâri a Congresului şi a studiat şi definit probleme referitoare la Protecţia Infrastructurilor Critice (CIP).

Intuitiv, înţelesul în limbajul natural al securităţii implică protecţia împotriva evenimentelor nedorite. Securitatea sistemului şi securitatea datelor sunt două tipuri de securitate. INFOSEC poate fi definită la două nivele. La nivel politic, INFOSEC reprezintă sistemul de politici, proceduri şi cerinţe de protecţie a informaţiei; la nivel tehnic, INFOSEC include măsuri şi controale ce protejează infrastructura informaţională împotriva interzicerii serviciului, pătrunderii neautorizate, şi modificării sau distrugerii componentelor infrastructurii informaţionale (inclusiv date). INFOSEC include totalitatea măsurilor de securitate necesare pentru a furniza un nivel de protecţie acceptabil pentru o infrastructură şi pentru datele vehiculate de o infrastructură.

Mai recent, aspectul de supravieţuire (capacitatea de

a face faţă atacurilor, şi de asigurare a funcţionalităţii la un anumit nivel de performanţă) a fost recunoscut că o componentă critică a apărării.

Este de dorit un sistem de ansamblu şi un set de cerinţe reale referitoare la conectarea largă în reţea, care presupun securitatea, încrederea, toleranţa la defectări, performanţa, şi orice alte atribute necesare pentru păstrarea unui sistem adecvat şi a supravieţuirii în reţea. Subiectul cel mai general al cerinţelor de securitate este dependabilitatea (în unele lucrări abordată că supravieţuire). Dependabilitatea (sau supravieţuirea) include cerinţe pentru componente (A) securitatea, (B) încrederea şi (C) performanţa.

Proprietăţile de bază ale securităţii sunt (1) confidenţialitatea, (2) integritatea, şi (3) disponibilitatea. Supravieţuirea este capacitatea unui sistem informaţional conectat în reţea de a satisface şi de a continua să satisfacă cerinţe critice certe (ex. cerinţe pentru securitate, încredere, răspuns în timp real, şi corectitudine) în faţa condiţiilor adversarului. Supravieţuirea trebuie să fie definită cu privire la setul de adversităţi ce suni presupuse că pot să existe.

Tipurile de adversităţi pot să includă în mod obişnuit defecte hardware, defecte soft, atacuri asupra sistemelor şi reţelelor carc conţin utilizatori necorespunzători, şi interferenţe electromagnetice. Deoarece este adesea făcută pentru încredere, supravieţuirea ar putea fi definită alternativ că o măsură probabilistică a cât de bine sunt satisfăcute anumite cerinţe date. Dar, de celc mai multe ori, este preferată o definiţie ne-cantitativă.

Există legături clare între conceptul de supravieţuire şi dependabilitate a sistemului. Cele trei atribute de bază ale securităţii sunt (1-3), şi sunt utilizate şi alte trei atribute suplimentare (4-6).

1. confidenţialitatea protejează existenţa unei conexiuni, fluxul traficului, şi informaţia împotriva dezvăluirii.

2. Integritatea asigură că informaţia şi procesele sunt

sigure împotriva accesului neautorizat prin metode cum ar fi criptarea, semnături digitale, şi detectarea pătrunderii.

3. Disponibilitatea furnizează asigurarea că informaţia şi serviciile vor fi accesibile şi utilizabile atunci când este nevoie.

4. Autenticitatea asigură că numai utilizatori autorizaţi au acces la informaţii şi servicii.

5. Ne-repudierea asigură că tranzacţiile sunt imune împotriva refuzului fals al trimiterii sau recepţionării de informaţii prin furnizarea unei evidenţe de încredere ce poate fi verificată independent pentru a stabili profilul originii şi livrării.

6. Restaurarea asigură că informaţia şi sistemele pol supravieţui unui atac şi că disponibilitatea poate fi refăcută după impactul unui atac.

Securitatea include atât securitatea sistemelor cât şi securitatea informaţiei. Trebuiesc anticipate toate ameninţările reale, incluzând utilizarea greşită de către utilizatorii din interior, penetrări de către utilizatorii din afară, interferenţa accidentală sau intenţionată (ex. electromagnetic), emanaţii, canale ascunse, inferenţă, şi agregări. Pentru a asigura securitatea este nevoie de mai mult decât de confidenţialitate, integritate şi disponibilitate.

Este nevoie de încredere, definită în general ca o măsură a cât de bine operează un sistem în cadrul specificaţiilor lui. De exemplu, toleranţa la defectări poate activa o varietate de alternative, incluzând moduri de operare în timp real, pierderea siguranţei, pierdere uşoară, pierdere rapidă şi pierderea securităţii. Performanţa este o cerinţă critică. În unele cazuri, performanţa adecvată poate fi critică pentru supravieţuirea unui sistem sau a unei aplicaţii.

Pe de alt parte, în cele mai multe cazuri, performanţa este ea însăşi dependentă de supravieţuire şi disponibilitate. Dacă un sistem nu supravieţuieşte, performanţa adecvată nu poate fi realizată. Ce este evident imediat este că există legături strânse între diferite

cerinţe.

Aici au fost rezumaţi paşii de securizare a sistemelor informaţionale conectate în reţea (figura 2) aşa cum au fost descrişi de Waltz. Analizele de securitate trebuie să fie aplicate pentru a determina gradul de risc al sistemului, pentru a identifica proiectarea, configuraţia, şi alte defecte şi vulnerabilităţi, şi pentru a verifica concordanţa cu politica şi modelul cerinţelor de securitate. Analizele pot să varieze de la o evaluare informală la o analiză de ansamblu şi exhaustivă.

Primul pas în procesul de analiză include o evaluare a ameninţărilor la adresa sistemului, bazată pe informaţii şi extrapolări ale capabilităţilor tehnologice. Evaluarea de vulnerabilitate presupune domeniile de acces posibil (intern şi extern) şi are în vedere vulnerabilitatea relativă (sau punctele slabe de lecuritate) corespunzătoare atacului. Vulnerabilităţile pot fi atribuite eşecurilor în analiza, proiectarea, implementarea, sau operarea unei reţele sau sistem.

Rezultatul evaluărilor ameninţărilor şi vulnerabilităţilor este o matrice a ameninţărilor ce clasifică ameninţările (prin categoria de atac) şi vulnerabilităţile (prin funcţii). Matricea furnizează o ierarhizare relativă a probabilităţii ameninţărilor şi a impactului posibil ale atacurilor adverse asupra fiecărei zone de vulnerabilitate. Aceste date formează baza pentru evaluarea de risc.

Procesul de management al riscului începe cu evaluarea riscurilor la sistemul care are asociată o matrice a riscurilor. Riscurile sunt cuantificate în termeni de probabilitate a apariţiei şi a gradului de impact nedorit dacă apariţia are loc. Pe baza acestei ierarhizări a riscurilor, este dezvoltată o abordare a managementului de risc ce îndeplineşte cerinţele de securitate ale sistemului.

Securitatea poate fi cuantificată în termeni de risc, şi includc patru componente: (1) procentul atacurilor detectate; (2) procentul detectat şi controlat; (3) procentul detectat, controlat şi recuperai şi (4) procentul de risc rezidual. Aceste faze introduc trei alternative de

management de risc.

(1) Riscul acceptat: Dacă ameninţarea este puţin probabilă şi impactul advers este nesemnificativ, riscul poate fi acceptat şi nu sunt impuse în continuare cerinţe de securitate suplimentare.

(2) Risc tratat (sau administrat): Dacă riscul este moderat, măsurile pot fi luate pentru a minimiza probabilitatea apariţiei sau a impactului nedorit sau a amândorura. Aceste măsuri pot să includă o combinaţie de OPSEC, TCSEC, INFOSEC, sau cerinţe interne de proiectare, dar efectul combinat trebuie să fie analizat pentru a obţine reducerea dorită a riscurilor în scopul îndeplinirii cerinţelor de sistem de nivel înalt.

(3) Risc evitat: Pentru riscurile cele mai drastice, caracterizate de probabilitate ridicată de atac sau de impact nedorit accentuat, sau de ambele, poate fi aleasă o abordare de evitare a riscului. Aici, sunt aplicate cele mai ridicate nivele ale proceselor de tratare a riscului (măsuri de securitate de înalt nivel) pentru a obţine o probabilitate suficient de scăzută la care riscul poate să aibă loc în operarea sistemului.

Când ameninţările şi vulnerabilităţile sunt înţelese, riscurile cuantificate şi măsurate sunt aplicate pentru a controla balanţa de risc, pentru a îndeplini util cerinţele de securitate de nivel înalt şi astfel administrarea în ansamblu a riscului sistem. Etapa de proiectare, apoi implementările proiectării, trebuie să fie subiect a analizelor de proiectare şi a testării pentru verificarea securităţii.

Suplimentar, o echipă roşie independentă poate fi aleasă pentru a conduce atacurile simulate asupra sistemului şi pentru a evalua performanţa de securitate actuală. Atacurile echipelor roşii (numite frecvent „teste de penetrare”) vizează securitatea fizică şi operaţională precum şi aspectele tehnice ale sistemului. Rezultatul verificărilor echipei roşii poate să se concretizeze în modificări de proiectare pentru a asigura corespondenţa cu cerinţele de securitate sistem.

La fel ca şi la securitatea şi siguranţa informaţională,

trebuie să ne gândim mai întâi la definiţii şi înţeles, deoarece războiul informaţional înseamnă un număr de lucruri diferite – probabil o combinaţie a tuturor acestora şi ceea ce înseamnă cu adevărat depinde de tendinţa particulară a cuiva. (1) Luptătorii informaţionali puri văd războiul informaţional ca un război fără bombe sati gloanţe; un conflict de orice magnitudine dus oriunde, independent de motivaţie. (2) Următorul grup crede în războiul informaţional. Mulţi dintre aceşti oameni simt că posibilităţile de luptă în război pot fi sporite prin aportul tehnologiilor informaţionale mai bune. (3) Războiul bazat pe cunoştinţe reprezintă o extrapolare inteligentă în devenire a ultimului concept fi face o distincţie între informaţie şi valoarea crescută subiectiv I cunoştinţelor. În cele din urmă, războiul informaţional reprezintă O convergenţă a problemelor de securitate militare şi civile şi a modului cum oamenii le tratează într-o lume în rapidă schimbare.

Obiectivul războiului bazat pe informaţii este în final realizarea de scopuri militare cu aplicarea cea mai eficientă a resurselor de informaţii. Operaţiile informaţionale ofensive sunt acte ce conduc la îndeplinirea obiectivelor strategice, operaţionale sau tactice ale corpurilor guvernamentale autorizate; organizaţiilor legale, criminale sau teroriste, corporaţiilor, sau ale indivizilor.

Atacurile informaţionale ofensive au două funcţii de bază: culegerea, respectiv afectarea informaţiei. Superioritatea informaţională reprezintă capabilitatea de a colecta, prelucra şi disemina un flux neîntrerupt de informaţii simultan cu exploatarea sau interzicerea posibilităţii adversarului să facă la fel. Dacă operaţiile informaţionale sunt realizate în contextul unei strategii, ele au un obiectiv dorit (sau stat final) ce poate fi obţinut prin influenţarea unei ţinte (obiectul influenţei).

Operaţiile informaţionale sunt definite de către Armata SUA ca operaţii militare continue în cadrul Mediului Informaţional Militar (MIE) ce activează,

îmbunătăţesc şi protejează capacitatea forţelor prietene de a colecta, prelucra, şi, utiliza informaţia pentru a obţine un avantaj în cadrul întregului domeniu al operaţiilor militare. Operaţiile informaţionale includ interacţiunea cu Mediu I Informaţional Global (GIE) şi exploatarea sau interzicerea informaţiilor şi capabilităţilor de decizie ale unui adversar.

Un model funcţional simplu este prezentat (figura 3) pentru a forma baza pentru discuţii viitoare ale operaţiilor şi tehnicilor angajate. Modelul este o extensie a modelului de conflict de bază şi include concepte ce evidenţiază trei domenii conceptuale ale activităţii de operaţii informaţionale.

Modelul evidenţiază că ţintele există în (1) spaţiul fizic, (2) cyber-spaţiu, şi (3) mintea oamenilor. Ţinta de nivelul cel mai înalt al operaţiilor informaţionale este percepţia umană a factorilor de decizie, oamenilor politici, comandanţilor militari şi chiar a întregii populaţii. Ţintele finale şi obiectivul operaţional este influenţarea percepţiei lor privind deciziile şi activităţile rezultate

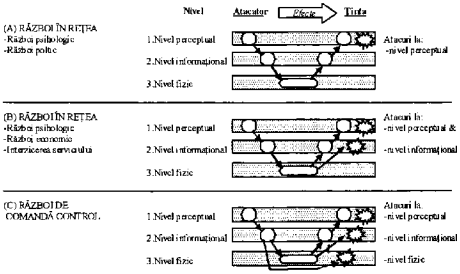


Figura 3: Modelul pe trei nivele al operaţiilor informaţionale

Modelul operaţiilor informaţionale (figura 3) distinge trei nivele sau straturi atât pe partea atacatorului cât şi pe cea a ţintei. Straturile sunt ierarhice, cu influenţă de sus în jos pentru atacator şi cu influenţă de jos în sus pentru ţintă. Obiectivul atacatorului este să influenţeze ţinta la nivel perceptual prin acţiuni ce pot avea loc la toate nivelurile ierarhiei. Cele trei nivele respecta modelul cognitiv, care conţine cunoştinţe la nivelul cel mai înalt,

informaţii la nivelul intermediar şi date la nivelul cel mai de jos.

Primul strat este la nivel perceptiv sau psihologic, care este de natură abstractă şi este orientat spre managementul percepţiei, pentru ţinta vizată. La acest nivel, obiectivul strategic defineşte acţiunile dorite ale ţintei şi percepţiile care vor determina cel mai probabil aceste acţiuni.

Dacă acţiunea dorită este determinarea agresiunii, de exemplu, percepţia obiectiv pentru conducătorii ţintă poate îi *„ajungerea la pierderea controlului, dezordine şi pierderea suportului populaţiei*" Dacă acţiunea dorită este neimplicarea într-(> acţiune militară, percepţia obiectiv pentru comandanţii militari poate fi *„lipsa de suport logistic pentru susţinerea operaţiei*" Aceste percepţii obiectiv pot fi realizate printr-o varietate de mijloace fizice sau abstracte (informaţionale), dar ţinta şi obiectivul final este numai la nivel perceptual abstract şi efectcle influenţează comportamentul operaţional.

Al doilea strat este stratul infrastructurii informaţionale care include infrastructura informaţională abstractă care accepţii, prelucrează, administrează şi stochează informaţia. Acesta este stratul care este considerat cel mai adesea că fiind dimensiunea de „cyberspaţiu" în care pot avea loc atacuri cu software dăunător şi atacuri de exploatare a infrastructurii (hacking). Atacurile pi* acest strat intermediar pot avea efecte specifice sau în cascadfl asupra straturilor perceptuale şi fizice.

Al treilea strat este nivelul fizic al sistemului, care include calculatoarele, reţelele fizice, telecomunicaţiile şi componentele structurale de sprijin (ex. tensiune, facilităţi, controlul mediului de lucru) ce implementează sistemul informaţional. De asemenea, la acest nivel se află administratorii umani ai sistemelor a căror influenţă fizică asupra sistemelor este determinantă. Atacurile la acest nivel sunt de natura fizică.

Atacurile pot să aibă loc direct asupra stratului

perceptual (ex. Întâlniri directe dintre lideri în care discursul uman este utilizat pentru a influenţa percepţia unei ţinte sau pentru a colecta informaţii) sau ele pot viza starturile de jos cu intenţia de a avea în consecinţă influenţe pe alte straturi.

Modelul ilustrează cum trebuiesc considerate elementele operaţionale la fiecare nivel al modelului. Să considerăm, de exemplu, cum trebuie considerată culegerea de informaţii pentru indicare şi avertisment, ţintire şi evaluarea pagubelor în luptă pe toate cele trei nivele.

În figura 3, sunt ilustrate ameninţările de atac prin modelul războiului informaţional pentru trei categorii de război informaţional. Exploatarea straturilor fizic şi informaţional, numai pentru scopuri de management al percepţiei sau război psihologic (PSYWAR), este ilustrată în partea de sus a figurii. Războiul de comandă şi control (C2W), în care atacurile au loc la toate trei nivelurile, este reprezentat în partea de jos a figurii.

Aceste distincţii sunt reprezentative numai prin acceptarea că în conflictele reale, atacurile vor avea loc pe toate nivelurile cu diferite grade de intensitate. Reţeaua de război la scară largă, de exemplu, poate fi susţinută de elemente la scară redusă dar cu atacuri fizice cruciale asupra infrastructurii sau personalului pentru a îndeplini obiectivele de ansamblu.

Pe parcursul ultimilor cinci la zece ani, à crescut interesul pentru protejarea infrastructurilor critice de care societatea depinde pentru a face faţă atacurilor fizice şi informaţionale. Organizaţia pentru Securitatea Sistemelor Informaţionale a NSA (NSA/ISSO) defineşte: *„Infrastructurile critice sunt acele sisteme fizice şi listeme bazate pe IT* (*tehnologia informaţiei*) *esenţiale pentru operaţiile minime ale economiei şi guvernului „*

Trebuie să considerăm diferite tipuri de infrastructuri: (1) infrastructuri critice naţionale, (2) infrastructuri informaţionale cum ar fi reţeaua Internet – sau orice poate s-o înlocuiască – o Infrastructură

Informaţională Naţională (NII), sau o Infrastructură Informaţională Globală (GII) -şi (3) software existent pe sistemele de calcul şi software de reţea. Este important din perspectiva prezentă acceptarea că există vulnerabilităţi şi ameninţări serioase asupra acestor infrastructuri critice. Poate la fel de important este acceptarea că aceste infrastructuri critice sunt interdependente îndeaproape şi că ele toate depind de infrastructurile de comunicaţie-calculator existente.

Pentru o anumită ţară, un set caracteristic de sectoare cu infrastructură critică pot fi găsite prin indentificarea atributelor ţării, structurii sale, organizaţiilor şi instituţiilor sale care contribuie inerent la bunăstare, şi determină o estimare a nivelului prezcnl de bunăstare.

Potrivit viziunii SUA, aceste infrastructuri subsumează iniţial opt sectoare majore: informaţii şi comunicaţii, energie electrică, finanţe şi bănci, apă şi canalizare, transport, petrol şi gaz, servicii de urgenţă (ex. poliţie, incendiu, medical) şi servicii guverna mentale de bază. Pe baza lucrărilor comisiilor, revizuirii, modificărilor uşoare şi agregării aceste sectoare au devenit cinei: (1) Informaţii şi comunicaţii; (2) Energie; (3) Bănci şi Finanţe; (4) Transport şi (5) Servicii Umane Vitale. Multe dintre aceşti* infrastructuri critice au devenit tot mai mult internaţionale. Aceasta este o consecinţă logică a creşterii globalizării.

Conceptul unei infrastructuri informaţionale de bază minima le (MEII) se referă la supravieţuirea şi asigurarea disponibilităţii unor infrastructuri informaţionale de bază, în special pentru a face lată formelor diferite de atacuri de război informaţional. Conceptul a fost propus în comunitatea infrastructurilor critice pentru a asigura că unele funcţionalităţi de bază ar putea să existe continuu în contextul unui domeniu rezonabil al ameninţărilor privind supravieţuirea – atacuri, îmbătrânire, eşecuri, disturbanţe de mediii şi aşa mai departe.

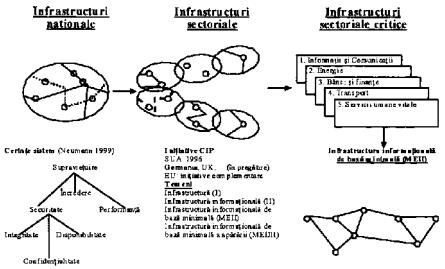


Figura 4: *Abordare pentru protecţia infrastructurii critice*

Până acum există o dezbatere considerabilă asupra definiţiilor de minimal şi de bază – precum şi asupra recunoaşterii problemelor inerente în încercarea de a concentra o singura MEII universală. Cu toate acestea, conceptul este valabil ca o ghidare a conceptului arhitectural. Bazată pe interviuri extensive, studii detaliate ale arhitecturi lor câtorva sisteme răspândite şi importante şi analiza de literatura privind vulnerabilităţile şi riscurile în sisteme informaţionale, a fost dezvoltată o metodologie de asistare pentru dezvoltarea baracteristicilor MEII în sistemele informaţionale viitoare.

Metodologia constă din (1) identificarea funcţiilor informaţionale ce sunt esenţiale pentru misiunea unităţii; (2) determinarea sistemelor informaţionale ce sunt esenţiale pentru îndeplinirea acestor funcţii; (3) căutarea vulnerabilităţilor în cadrul acestor componente de sisteme; (4) aplicarea tehnicilor de protecţie adecvată pentru vulnerabilităţile găsite la diferite niveluri ale sistemului şi (5) testarea protecţiilor împotriva unui set de scenarii de ameninţare pentru a verifica robusţetea lor. Aplicarea acestei metodologii va avea că rezultat o formă de MEII ce este un set de sisteme în structuri implicate de securitate sporită.

Scopul unei infrastructuri pentru asigurarea cercetării şi dezvoltării (R&D) este de a susţine dezvoltarea tehnologiilor care vor contoriza ameninţările şi vor reduce vulnerabilităţile în acele domenii ce au potenţialul unui impact semnificativ asupra securităţii

naţionale, economiei şi societăţii. Sunt avute în vedere ameninţările fizice şi informaţionale. Tehnologiile considerate specifice sunt acelea care protejează infrastructura şi astfel redue vulnerabilitatea, detectează intruziunile şi furnizează avertismente, tratează efectele de disfuncţionalităţi (incidente), asigură asistenţă pentru managementul incidentelor şi facilitează recuperarea.

Punctele focale ale programului sunt: (1) dezvoltarea tehnologiilor ce susţin recunoaşterea rapidă a atacurilor la scară mare, (2) dezvoltarea sistemelor ce înglobează inerent caractc ristici de supravieţuire, de exemplu capacitatea de a continua operarea în situaţia atacurilor ce au succes parţial. Obiectivele specifice sunt: (a) recunoaşterea atacurilor la scară naţională şi distingerea lor de evenimentele cu semnificaţie locală; (b) limitarea impactului unui atac prin asigurarea integrităţii datelor şi programelor; şi (c) împiedicarea atacurilor de interzicere a serviciului prin limitarea consumului de resurse ce poate fi făcut de un atacator. În final, trebuie să realizăm că multe dintre infrastructurile critice devin tot mai mult internaţionale. Aceasta este o consecinţă logică a creşterii globalizării.

Între timp, câteva iniţiative de protecţie a infrastructurilor critice sunt în pregătire în Europa (ex. Uniunea Europeană, Germania, UK). Complementar cu iniţiativele naţionale în Europa, Comisia Europeana studiază stabilirea unei Iniţiative de Dependabilitate Europeană ale Programului de Tehnologii Informaţionale pentru Societate.

Această activitate este îndeplinită cu ajutorul Centrului de Cercetare Integrat, Institutului pentru Sisteme, Informatică şi Siguranţă. Studiile iniţiate de Comisia Europeană introduc şi explorează conceptul de supravieţuire. El evidenţiază distincţia între perspectiva de dependabilitate tradiţională şi punctul de vedere curent studiat în prezent în domeniul supravieţuirii.

Raportarea şi analizarea incidentelor de securitate va rămâne pentru mult timp o problemă nerezolvată, dacă

numai un atac din 20 este reţinut de către victimă şi numai un atac din 20 este raportat, într-un studiu neobişnuit de larg şi de stringent, Howard a analizat tendinţele în domeniul securităţii Internet printr-o investigare a 4299 de incidente de securitate pe Internet raportate de Centrul de Coordonare CERT (CERT/CC) din 1989 până în 1995

Înainte de această cercetare, cunoştinţele noastre despre problemele de securitate pe Internet au fost limitate şi în principiu doar anecdote. Cercetarea desfăşurată de Howard a îndeplinit Următoarele: (1) dezvoltarea unei taxonomii pentru clasificarea atacurilor şi incidentelor Internet, (2) organizarea, clasificarea şi analiza înregistrărilor incidentelor raportate de CERT/CC şi (3) dezvoltarea recomandărilor pentru îmbunătăţirea securităţii, Internet şi pentru obţinerea şi distribuirea informaţiilor despre securitatea Internet.

Cu excepţia atacurilor de interzicere a serviciului, incidentele de securitate au fost găsite în general ca fiind în descreştere relativ la dimensiunea Internet. Estimările bazate pe această cercetare că un domeniu Internet obişnuit a fost implicat în medie la un incident pe an şi un post Internet obişnuit a fost implicat într-un incidenl odată la 45 de ani.

Taxonomia atacurilor asupra calculatoarelor şi reţelelor dezvoltată în această cercetare a fost utilizată pentru a prezenta un rezumat al frecventei relative al diferitelor metode de operare: şi a acţiunilor corective. Aceasta a fost urmată de o analiză a trei subgrupuri: (1) un studiu de caz a unui site care a raportat toate incidentele, (2) 22 de incidente care au fost identificate în înregistrări, prin diferite metode, ca fiind cele mai severe şi (3) incidente de interzicere a serviciului.

Datele de la toate incidentele şi de la aceste trei subgrupuri au fost folosite pentru a estima întreaga activitate de incidente Internet pe timpul perioadei de cercetare. Aceasta a fost urmată de o evaluare critică a utilităţii taxonomiei dezvoltate prin această cercetare.

Analiza concluzionează cu recomandări pentru

utilizatorii Internet, furnizorii Internet, echipele de răspuns şi guvernul SUA. Studiul lui Howard prezintă numai o analiză preliminară a datelor rezultate din înregistrările incidentelor în perioada 1989-1995. A fost recomandat că setul de date ar trebui făcut disponibil on-line pentru utilizarea de către alţi cercetători. Suplimentar, informaţii referitoare la analiza incidentelor, problemele metodice asociate şi utilizarea taxonomiilor este oferită de Cohen.

Corelat cu creşterea incidentelor de securitate, a apărui criminalitatea în domeniul calculatoarelor şi utilizarea greşită, depinzând fără îndoială de proliferarea tehnologiilor de calcul şi creşterii Internet. Partea din stânga a figurii 5 evidenţiază număru I de raportori ce au raportat diferite tipuri de atacuri sau de utilizare greşită relativ la resursele lor de calcul şi telecomunicaţii, ordonate de la cel mai preponderent la cel mai puţin preponderent.

Partea din dreapta a figurii 5 prezintă pierderile în mii de dolari pentru incidente de aceste tipuri cu pierderi cuantificabile. Figurile arată că deşi au fost contorizaţi viruşi de cel mai mare număr al companiilor, 73% din raportori spunând că au detectat incidentele de acest tip, ele nu au contabilizat pierderile cele mai mari, care au fost atribuite accesului neautorizat de către utilizatori din interior şi furtului de informaţii proprietar.

Ultimele două ameninţări raportate, ascultarea activă şi pasivă, a fost contabilizată pentru pierderi mici. Raportorii au spus că sursele cele mai probabile ale atacurilor sunt angajaţii nemulţumiţi (80%), hackerii independenţi (72%), corporaţiile din (ară (48%), corporaţiile străine (29%) şi guvernele străine (21 %).

Siguranţa informaţională include totalitatea măsurilor de securitate necesare pentru a furniza un nivel de protecţie acceptabil pentru o infrastructură şi pentru datele vehiculate de o infrastructură. Mai recent, aspectul de supravieţuire a fost recunoscut ca o componentă critică. Supravieţuirea sistemelor include caracteristici de:

toleranţă la defectări; robusteţe, răspuns adaptiv; distribuţie şi variabilitate; recuperare şi restaurare.

În acest capitol, accentul se pune pe măsuri de securitate tehnică, dar şi măsurile de securitate fizică şi de personal sunt esenţiale pentru protecţia complementară. Securitatea la nivel fizic include controale pentru accesul fizic la facilităţi, protecţia de eşecul utilităţilor de sprijin, dezastre naturale şi multe alte ameninţări.

Un model de politică de securitate formal reprezintă partea centrală a conceptului de încredere. El defineşte matematic o bază de calcul de încredere (TCB) ca un model abstract.

Modelul include noţiunea de securitate a stării pentru TCB, subiecţi (utilizatori ce accesează TCB), obiecte (seturi de date în TCB) şi acţiuni pe care TCB le realizează. Modelul descrie aceste acţiuni fundamentale şi starea tranziţiilor TCB. Modelul permite analiza şi furnizează un mijloc de dovedire că orice implementare a arhitecturii TCB rămâne întotdeuna într-o stare stabilă.

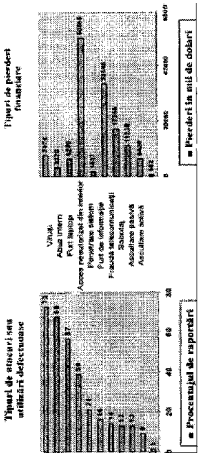


Figura 5: Criminalitate în domeniul calculatoarelor: Tipul de atac şi pierderi financiare

Controlul accesului pentru autentificarea utilizatorilor reprezintă mecanismul de securitate fundamental a unui singur sistem sau a unor sisteme în reţea. Procesul de autentificare impune utilizatorului

verificarea identităţii pentru a stabili accesul şi restricţiile de control al accesului, procesele ce pot fi realizate de utilizatorul autentificat sau utilizatorii ce încearcă obţinerea autentificării. Autentificarea unui utilizator într-o manieră sigură necesită un mecanism ce verifică identitatea utilizatorului la gradul de siguranţă dorit.

Criptografia furnizează procesele matematice pentru transformarea datelor (prin criptare şi decriptare) între un format deschis şi un format de text cifrat pentru a furniza proprietăţi private. Puterea algoritmului de criptare reprezintă o măsură a gradului în care textul cifrat suportă atacurile. Puterea finală şi generalitatea prelucrărilor criptografice stă în formularea matematică a algoritmilor de transformare utilizaţi.

Sistemul de criptare general include calea la mesajul criptografic ce include procesul de criptare, transmisie şi decriptare şi o metodă suport pentru distribuirea unei variabile numerice, sau chei, care controlează transformarea de criptare. Generarea, stocarea, distribuirea şi protecţia de ansamblu a cheilor sunt critice pentru securitatea tuturor cripto-sistemelor. Cheile compromise furnizează mijloacele cele mai directe pentru accesul neautorizat. Din acest motiv, nivelurile de securitate fizic, informaţional şi perceptual trebuie să protejeze funcţiile de management a cheii, incluzând pe cele sintetizate mai jos. Suplimentar furnizării de intimitate, procesul de criptare furnizează un mijloc de autentificare a unui mesaj printr-un element de criptare a datelor numit semnătura digitală. Semnătura digitală permite dovedirea identităţii expeditorului şi dovedeşte că atacatorul nu a modificat mesajul.

Zidurile de foc sunt sisteme de încredere care integrează autentificarea, controlul conexiunii, răspunsul la incidente, criptarea, securitatea structurii de reţea şi conţinutul de securitate într-o singură unitate de securitate. Localizat între două reţele, loi traficul de trecere între reţele trebuie să treacă prin zidul de loc, care restricţionează trecerea numai celor ce le este permis

traficu I prin politica de securitate.

Zidul de foc creează efectiv un „domeniu” de securitate sau o „enclavă”, prin furnizarea unui perimetru de apărare pentru n reţea (domeniul securizat). Cele patru tipuri de bază ale zidurilor de foc sunt (1) filtre de pachete, (2) bazate pe circuite, (3) porţi de aplicaţie şi (4) filtre pachet dinamice.

Sistemele pentru detectarea intruziunii şi răspunsului (IDS) sunt necesare pentru a proteja sistemele de calcul şi reţelele de intruziuni interne sau externe. Securitatea calculatoarelor tradiţională face distincţia între activitatea de verificare şi cea de raportare a alarmării.

Verificarea de securitate revizuieşte înregistrările activităţilor pentru a detecta incidentele de securitate (incluzând schimbări în configuraţia operaţională), pentru a verifica corespondenţa cu politica de securitate şi a testa controalele de securitate. Raportarea alarmării de securitate monitorizează evenimentele legate de securitate care pot indica utilizarea greşită a controalelor sau configuraţiilor de securitate, activităţi ostile împotriva controalelor de securitate sau comportamente inconsistente cu politica de securitate.

Detectarea automată a incidentelor, respectiv, raportarea şi răspunsul de alarmare este necesar pentru a răspunde la atacuri de război informaţional structurate asupra reţelelor. La fel ca în toate sistemele de alarmare, alarma falsă şi ratele de detectare greşită măsoară în ansamblu performanţa de detecţie. Detecţia automată şi raportarea este necesară pentru un domeniu larg de acţiuni de ameninţare, ex. intruziuni externe, intruziuni de securitate internă, eşecuri de sistem şi comportare ciudată.

Cetăţenii, industria, guvernul şi militarii au devenii vulnerabili datorită bazării pe tehnologie, în particular tehnologii informaţionale. Mai temător chiar, dar mai puţin înţeles, este c;

această vulnerabilitate este sporită datorită bazării

pe economia mondială şi aranjamentelor de coaliţie în domeniul militar. Deoarece imensitatea problemei siguranţei informaţionale (IA) în faţa societăţii informaţionale este neacoperită, o atenţie sporită este acordată acestui subiect de către presă, industrie şi guvern.

Domeniul siguranţei informaţionale se concentrează pe proiectarea sistemelor care poate să determine politici de securitate chiar în prezenţa codului dăunător. Provocarea este de a proiecta, dezvolta şi răspândi sisteme complexe cu încredere în posibilitatea lor de a satisface cerinţe de securitate. Este în curs de dezvoltare o teorie a securităţii calculator care oferă o metodă formală pentru ingineria de securitate, aşa încât ne putem aştepta să obţinem tehnologii accesibile, verificabile, scalabile pentru o infrastructură a apărării robustă şi sigură. Această teorie va avea trei componente: politica, mecanismul şi siguranţa.

Au fost făcute încercări pentru a aborda problema în creştere a siguranţei informaţionale. Unele dintre aceste încercări au fost tipic „reacţionare”, la nivel de suprafaţă, şi cu concentrări înguste. De exemplu, zidurile de foc au fost introduse pentru a proteja reţelele de arie locală din Internet, oricum ele au fost dezvoltate la nivel superficial pentru a controla protocoalele şi ameninţările cunoscute care apăreau evidente. Mulţi autori au arătat că există probleme inerente în procesele de proiectare şi evaluare existente care creează sistemele noastre informaţionale.

În concordanţă cu DARPA, aceste probleme pot fi abordate numai printr-o schimbare fundamentală în filosofia de siguranţă informaţională. Este evident că metodele existente sunt inconsistente, ineficiente, nu abordează problemele dintr-un punct de vedere cu adevărat „la nivel sistem” şi au scopuri şi rezultate limitate de natură în prezent abstractă şi imatură a disciplinei. Aceste limitări nu pot fi depăşite cu cercetare de evoluţie suplimentară în aceleaşi concepte cheie ca cele ale vulnerabilităţilor, ameninţărilor şi contramăsurilor.

În concordanţă cu DARPA este necesară o nouă paradigmă de siguranţă informaţională – ceva ce face posibil pentru proiectant şi analist să culeagă şi să probeze cauzalitatea, legăturile, şi obiectivele întregului sistem. Un pas în ştiinţa de bază a siguranţei informaţionale ar trebui să fie dezvoltarea de echivalenţe, legături, legi, logici, postulate, dovezi şi metode de calcul aşa încât metrici le să poată fi utilizate efectiv.

La fel ca în alte discipline, complexitatea sistemelor nu va li permisă pentru soluţii închise, astfel va fi necesară modelarea siguranţei informaţionale. Scopul general al noii abordări DARPA este de a furniza un mediu ştiinţific pentru proiectare şi evaluare care va duce la siguranţă informaţională îmbunătăţită şi va permite proiectarea şi evaluarea mai rapidă la costuri mai mici. Acest mediu va consta din metode şi mijloace automate ce furnizează rezultate şi matrici consistente de evaluare a siguranţei informaţională.

Această muncă este realizată deoarece oamenii ce lucrează în prezent în domeniul proiectării şi evaluării nu au nicio cale de a măsura consistent multe aspecte ale siguranţei informaţionale. Ei lucrează de asemenea fără un mediu integrat şi un suport de unelte automate ce ar putea îmbunătăţi pe scară largă performanţa lor şi siguranţa sistemelor lor informaţionale.

Unele analize ale metodelor şi uneltelor necesare comunităţii de război informaţional (IW) au avut ca rezultat un set important de descoperiri şi recomandări. Evaluarea naturii problemei a condus la aprecierea că metodele de război informaţional trebuie să fie în măsură să opereze cu procese complexe, dinamice, interactive şi adaptabile, echipe de oameni sub stress, de culturi diferite şi incertitudine ca o proprietate inerentă. S-a anticipat că va fi necesar un amestec divers de metode şi tehnici pentru a ataca problemele din domeniile IW.

Aceste metode bazate pe unelte ar trebui să includă, dar nu să se limiteze la următoarele: (1) Expert în sinteză (ex. utilizarea mijloacelor structurate pentru judecăţi de

sinteză ale experţilor); (2) Modelare şi Simulare Constructivă (ex. Operatori simulaţi ce operează sisteme simulate); (3) Modelare şi Simulare Virtual;

(ex. Operatori reali ce operează sisteme simulate); (4) Modelare şi Simulare Efectivă (ex. Operatori reali ce operează sisteme reale).

Realizarea educării profesionale în domeniul războiului informaţional (IW), siguranţei informaţionale (IA), şi protecţiei infrastructurii critice (CIP) reprezintă o nevoie urgentă în toate organizaţiile civile şi militare ale tuturor ţărilor deoarece cel mai important aspect al acestor trei domenii îl reprezintă oamenii. Pentru a face faţă acestor provocări trebuie să îmbunătăţim atât calitatea cât şi realizarea unei educaţii corespunzătoare.

Numărul personalului instruit special pentru securitatea sistemelor de calcul care pot să abordeze complexitatea tehnologiilor moderne şi care sunt familiari cu abordările de securitate a sistemului este foarte redus.

Oamenii doresc securitatea, dar sunt confruntaţi cu două dificultăţi. Mai întâi, ei nu ştiu cum să o obţină în contextul întreprinderii lor. Ei poate chiar nu cunosc o modalitate de a translata procedurile organizaţionale în politici, cu atât mai puţin implementarea unui set de mecanisme pentru a forţa aceste politici, în al doilea rând, ei nu au nicio modalitate de cunoaştere dacă mecanismele alese de ei sunt eficiente. Abordările educaţionale moderne evidenţiază siguranţa informaţională nu ca o simplă disciplină separată, ci ca o ştiinţă multi-disciplinară care include elemente ale sistemelor de operare, reţelelor, bazelor de date teoriei de calcul, limbajelor de programare, arhitecturii şi interacţiunii om-calculator, încorporate ca apropiate în acest set de discipline.

În 1999 Organizaţia pentru Securitatea Sistemelor Informaţionale a NSA (NSA/ISSO) a fondat un Program Naţional de Instruire şi Educaţie INFOSEC (NIETP) cu şapte subprograme: (1) Şapte Centre de Excelenţă Academică în educaţia de siguranţă informaţională; (2) Colocviul Naţional pentru Educaţia de Securitate a

Sistemelor de Calcul; (3) Programul Universitar Extins; (4) Programul Curriculum – A – de Dezvoltare Electronică; (5) Iniţiativa „Cutia Albastră”; (6) Programul de Consultare Profesorală a Serviciului Academic; (7) Cursuri de Siguranţă Informaţională şi de Evaluare a Proceselor.

Obiectivele Colocviului Naţional sunt de a crea un mediu pentru schimbul şi dialogul între liderii din guvern, industrie şi academii, referitor la nevoia şi utilitatea educării în domeniul securităţii şi siguranţei informaţionale. Dat fiind scopul şi starea fluidă a cunoştinţelor despre securitatea informaţională, Colocviul va încerca să promoveze dezvoltarea preocupărilor academice care recunosc nevoia exprimată de guvern şi industrie, şi este bazată pe „cele mai bune practici” disponibile în domeniu. Colocviul va asista instituţiile educaţionale pentru promovarea dezvoltării continue şi partajarea resurselor educaţionale de securitate informaţională.

Cursul de război informaţional (IW) al Şcolii Postuniversitare Navale (NPS), Monterey, este proiectat pentru a furniza studenţilor posibilitatea de a aplica analiza şi teoria inginerească de sistem, fundamentală pentru probleme sistem de IW întâlnite într-un mediu operaţional. Studenţii pot modela un sistem informaţional generic, pot aplica teoria de proiectare inginerească a sistemelor şi pot face prelucrări pentru a dezvolta un sistem de IW relevant.

Ei ar putea să înveţe să aleagă abordări ce par inginereşti pentru a apăra sistemul aflat în studiu şi respectiv pentru a ataca sistemul dacă se presupune posesia lui de către un adversar. Cursul poate fi coordonat utilizând pas cu pas procesul de analiză a deciziei. De exemplu, analizele căilor nodale şi critice pot fi revizuite pentru vulnerabilităţi, cu accent pe tendinţele tehnologice în domeniile comunicaţiilor şi calculatoarelor.

Sistemele de decizie organizaţională (comandă şi control) şi ingineria factorilor umani va fi studiată în scopul de a permite modelarea adversarilor militari şi

structurii de comandă civile ca parte a proiectului. Poate fi un proiect de curs (cu două echipe în competiţie) destinat pentru formularea şi prezentarea sistemelor unei organizaţii, pentru rezolvarea aplicaţiilor operaţionale specifice provocărilor de război informaţional, utilizând echipamentul de comunicaţie selectat.

CONCLUZII

Cu douăzeci de ani în urmă, infrastructurile informaţionale ale corporaţiilor şi cele militare erau separate şi distincte şi termenul de „război informaţiona144 nu exista. Astăzi ele sunt pe cale să devină unul şi acelaşi, şi sistemele informaţionale conectate în reţea rezultate, deschid multe uşi pentru războiul informaţional. Comunitatea militară depinde de aceleaşi (sau aproape aceleaşi) reţele de calcul şi echipamente de reţea pentru a lupta în războaie cu cele de care depinde sectorul industrial pentru a conduce afacerile.

În acest scop, este important de subliniat că peste 95% din legăturile de comunicaţie ale SUA utilizează linii şi sateliţi comerciali, închiriaţi şi pe timpul operaţiunii Furtună în Deşert, procentul a fost chiar mai mare. Guvernul are trei roluri referitoare la infrastructura informaţională naţională: să fie gata să facă faţă ameninţărilor iminente, să impună reguli adecvate, să promoveze confidenţa publică. Această lucrare ar putea să ajute la deschiderea unui dialog între academie, industrie şi guvern, înspre asigurarea infrastructurilor informaţionale şi sistemelor informaţionale.

Comunitatea de securitate are nevoie de un vocabular comun pentru a discuta ameninţările şi contramăsurile, şi o metodologie comună de descoperire a vulnerabilităţilor din sistem, stabilirea unei priorităţi în termeni de pericole relative şi determinarea costului efectiv al contramăsurilor.

Astfel, există un domeniu de probleme comune în contextul războiului informaţional, cu provocări pentru un nou nivel de cooperare în ştiinţă, inginerie, şi educaţie –

dar multe dintre aceste probleme continuă să rămână nerezolvate pentru cooperare. Aşa cum s-a prezentat în figura 1, domeniile războiului informaţional (IW), securităţii informaţionale (INFOSEC), şi protecţiei infrastructurii critice (CIP) sunt împreună şi ar trebui să lucrăm ţinând cont de inter-legături le dintre subdomeniile lor.

RĂZBOIUL CUNOAŞTERE
RICHARD SZAFRANSKI

Tezele dezvoltate aici se referă la cât de mult mai au de învăţat militarii şi autorităţile naţionale despre integrarea efectivă a operaţiilor informaţionale în operaţiile de securitate, pe timp de război sau de pace. La nivelul actual, la care se găsesc democraţiile vestice şi cele nou admise în Uniunea Europeană, acestea pot ceda în faţa acelor state, hackeri sau criminali care se adaptează mai repede la aceste instrumente. Acestea fiind spuse, nu intenţionez ca acest material să devină echivalentul cărţii „Al treilea val”. Cu toate acestea, este un material care cheamă la acţiune.

Războiul informaţional ofensiv, utilizează, pe scurt, tehnologiile informatice şi alte capacităţi pentru a ataca infrastructurile bazate pe informaţii ale adversarului. „Comisia preşedintelui SUA privind protecţia infrastructurii critice” este îngrijorată de echipamentele speciale cerute pentru a lansa atacuri RI asupra sistemelor de calculatoare americane. Instrumentele de atac de bază (calculatorul, modemul, telefonul NET-ul şi programele software) sunt, în general, aceleaşi cu cele pe care le utilizează hackerii şi criminalii. Comparându-le cu forţele militare şi armele care ameninţau în trecut infrastructurile americane, instrumentele RI sunt ieftine şi rapid de obţinut[79].

Mişcarea de la ceva vechi şi familiar, spre ceva nou şi necunoscut, este un proces dificil pentru oricine şi mai ales pentru infanterişti, marinari şi aviatori. După cum remarca

79 Comisia preşedintelui SUA privind protecţia infrastructurii critice, p. 30.

Hart, nimic nu e mai greu decât o înlocuire a vechilor idei. Atunci când infanteriştii, marinarii, şi aviatorii cred că au ajuns să ştie totul despre arta operaţiilor, o nouă descoperire (de obicei tehnologică sau o aplicaţie) transformă elementele considerate până acum nesemnificative. Când se întâmplă acest lucru, Zeul Marte se bucură. Trebuie să privim în trecut pentru a vedea viitorul.

Imaginaţi-vă cât de greu trebuie să le fi fost militarilor să accepte şi să se acomodeze cu tehnologiile artificiale ale armelor de foc şi ale tunurilor. A înjunghia, a răni, a zdrobi victima pare să mimeze vânătoarea perfectă, iar vânătoarea în haită sau pluton este o activitate care poate fi naturală speciei noastre. Noile competenţe în chimie, metalurgie, inginerie, au trebuit să se dezvolte în tandem cu noi organizaţii şi scheme de angajare. Armele de foc şi tunurile au schimbat modul de a vâna al oamenilor. Armele de foc au constituit unul dintre elementele care au condus la transformarea corăbiilor, vapoarelor. Vapoarele cu aburi le-au înlocuit pe cele cu pânze, motoarele au înlocuit vaporii, doar pentru a vedea întoarcerea acestora sub forma puterii nucleare. Vapoarele au fost martorele creşterii influenţei zonei subacvatice, în timp ce avioanele au devenit mesagerul câmpului de luptă aerian, ca principal mijloc de putere, de protecţie.

Tehnologia aparaturii cu combustie internă şi aplicaţiile sale terestre au înlocuit caii şi au condus la o reinterpretare a strategiei războiului. Şi atunci au apărut maşinile zburatoare în nenumăratele lor variante. Armata încearcă permanent să se adapteze.

Însă atunci apar rachetele şi armele nucleare, şi spaţiul cosmic Cercetările germane asupra vehiculelor destinate să poarte arme Convenţionale ne-au dat rachete balistice şi de croazieră. Armele nucleare au dat acestor rachete energia necesară. Armele de precizie de lungă distanţă, nucleare sau nu, care se autoghidează, permit forţelor armate să stea departe de câmpul de luptă şi să provoace pierderi adversarului. Toate forţele armate

doresc aceste arme convenţionale sau nu şi le folosesc într-un mod atât de mare încât ar şoca un om de rând.

Armele de precizie care acţionează la distanţă reprezintă acum *lingua franca* a războiului. Forţele armate se ceartă, au opinii diferite în privinţa a ceea ce înseamnă acest lucru pentru război, pentru misiunile lor separate, pentru diferenţierea operaţiilor în mediile „lor" şi pentru rolul forţelor aeriene şi cosmice. Forţele terestre, aeriene şi navale încearcă să ocolească aceste schimbări, şi mărturie stau dezbaterile care precedă orice operaţie semnificativă. Însă armatele ştiu că noţiuni, ca „puterea de a zbura", depăşesc puterea de acceptare a publicului versus „operaţii sângeroase". Voinţa de a se angaja formal în astfel de operaţii aşează armatele mai aproape de putere. Chiar şi armatele apreciază că riscul real la care se expune o ţară în lumea de azi nu este invazia unei alte armate, ci puterea de a zbura şi terorismul. Puterea de a zbura devine azi forţa dominantă?

Nu. Adevăratul risc nu mai sunt armele de precizie şi nici vehiculele zburătoare, ci noile descoperiri. Acestea, gravitând în jurul ideii de „noutăţi intangibile" nu elimină vechile „mijloace" de luptă, însă le permit să se dezvolte sau, în unele cazuri, să fie înlocuite de noile descoperiri. Toffler a scris că: „Nimic nu sugerează că resursele şi tehnologiile materiale vor dispărea. Evident, lucrurile contează, şi mai ales armele. Software are încă nevoie de hardware. Soldaţii nu pot mânca date. Şi legăturile fundamentale dintre instrumentele tangibile şi ceea ce am putea numi „noile instrumente intangibile" sunt cruciale pentru eficienţa militară, în ducerea războiului, cât şi în încercarea de a-l preveni"[80].

Războiul informaţional este noua mare descoperire pe care acoliţii Zeului Marte trebuie s-o întâmpine. Marte, doar „ne-a dar computerele, iar acestea „ne-au învăţat" că tot ce ne înconjoară poate fi redus la o combinaţie de zero

80 A. şi H. Tofiler, „Foreward: The New Intangibles", In Athen n \ Camp: Preparing for the Conflict in the Information Age, RAND, 19()1

şi unu. Această înţelegere a lansat epoca informaţională, în care aceste combinaţii pot l i transmise electronic ca date şi recombinate de cel care le primeşte:, pentru a forma bazele unei informaţii. După părerea lui Arquilla şi Ronfeldt, „informaţia" reprezintă mai mult decât conţinutul sau înţelesul unui mesaj, „informaţia este orice diferenţă care face diferenţa"[81]. Ameninţarea faptului că aproape orice poate avea semnificaţie militară în lumea exterioară, a lansat epoca războiului informaţional.

Războiul informaţional este dificil să devină apanajul unor instituţii, deoarece este o modalitate de acţiune indirectă şi subtilă şi nu una directă şi brutală. Războiul informaţional este o formă a conflictului, care atacă sistemele informaţionale (carbonul şi siliconul ca *mijloace* de atac al cunoştinţelor sau crezurilor adversarului). Războiul informaţional poate fi văzut că o componentă a unor activităţi ostile mai mari (ceea ce Arquilla şi Ronfeldt numesc *net war* sau *cyberwar*) sau poate fi înţeles ca unica formă a unei activităţi ostile. Războiul informaţional se poate duce *în timpul* războiului sau *în afara* lui.

Să citim cu atenţie ceea ce promovează US Force ca doctrină. Potrivit US Force, războiul informaţional cuprinde acele „(...) operaţii informaţionale care sunt executate pentru a-şi apăra propriile informaţii şi sisteme informaţionale, afectând informaţia adversarului şi sistemele sale informaţionale. Aspectul defensiv este operaţional în permanenţă. În schimb, aspectul ofensiv este, În primul rând, pus în aplicare pe timp de criză şi de conflict. Războiul informaţional include diverse activităţi ca operaţii psihologice, înşelare militară, război electronic, atacuri fizice şi informaţionale şi o serie de activităţi şi programe de apărare. Este important să se accentueze faptul că *războiul informaţional* este o Construcţie care se execută de-a lungul întregului spectru, de la pace la război, pentru a permite aplicarea efectivă a

81 J. Arquilla şi D. Ronfeldt, „Cyberwar is Coming!", Comparative Strategy 2, 1993. '

responsabilităţilor Forţelor Aeriene”[82].

Războiul informaţional cuprinde operaţiile informaţionale duse pentru a apăra propriile informaţii şi sisteme informaţiona lisau pentru a ataca şi afecta informaţiile şi sistemele informaţionali ale adversarului. Acest război e condus în primul rând pe timp de criză şi conflict. Totuşi, componenta defensivă, mai mult decât ofensiva aeriană, e condusă de-a lungul spectrului, de la pacc la război”[83].

Războiul informaţional ofensiv, „contra-informaţiile ofcn sive” cum le numeşte USAF, sunt duse *în primul rând*, dar nu *exclusiv* „pe timp de criză sau conflict”. Acest tip de război e *nou* şi noutatea a fost întotdeauna o provocare.

Nu este nevoie de panică, ci doar de a lua lucrurile în serios O motivaţie puternică pentru schimbare se cuvine să fie avertizarea privind perturbaţiile serioase pe care le poate aduce războiul informaţional doar prin încercarea de a modifica câmpul de lupta Orice tulburare serioasă în sistemele informaţionale poate reducieficienţa operaţiilor. Să analizăm cunoscuta de acum problema Y2K [84]. Aşa cum spunea şi senatorul Robert Bennett, vorbind despre această problemă, „antidotul panicii este informaţia curata, dar anumite informaţii curate pot fi infricoşatoare”[85].

La un nivel mai redus al agravării, grupuri mici sau state pot utiliza războiul informaţional pentru a dezbina o mare parte a funcţiilor unui alt stat. La un nivel mai ridicat, grupurile mici sau statele pot afecta serios marile state[86]. Aceştia pot duce un, jăzboi informaţional strategic”

---

82 United States Air Force, „Information Operations", Air Force Poctrine Document 2-5, 05.08.1998.

83 Air Force Doctrine Document2-5.

84 Andrew Hay, „Top Y2K problem: Public Panic", Reuters, 22.06.1999.

85 Jim Abrains, „Spreading the Y2K word without spreading panii " 08.06.1999, www.nandotimes.com

86 A se vedea The President's Commission on Criticai Infrastruktur Protection, pag 30, oct. 1998.

sau pot poseda capacităţi de „război informaţional strategic”. Capacităţile strategice sunt cele care pol da „lovituri serioase” securităţii altora sau securităţii intereselor altora.

Dacă contra-războiul informaţional ofensiv poate fi dus în afara războiului, războiul informaţional strategic poate fi şi el realizat fără o declaraţie de război[87].

De aceea, trebuie să ne pregătim pentru astfel de acţiuni încă de acum, deşi „Defensive Science Board” a estimat încă din noiembrie 1996 că avem ceva timp la dispoziţie: „capacităţile de război informaţional strategic” utilizate împotriva noastră se află încă la o distanţă de şapte-zece ani depărtare[88]. Aşa să fie?

Un studiu al RAND notează că: „O evaluare macro a stadiului primei generaţii a războiului informaţional strategic al SUA şi al altor state (sau a altor părţi), în termeni de capacităţi absolute şi relative de război informaţional strategic ofensiv şi defensiv ar fi dificil de realizat, chiar şi la un nivel secret. Caracterul dinamic actual al revoluţiei informaţionale şi caracterul embrionar al războiului informaţional strategic ca potenţial instrument politicomilitar, conduc la ideea unei abordări mai precaute în a face o astfel de evaluare, secretă sau nu, pentru prezent sau viitor”[89].

Fără a pune un mare accent pe „viitor”, aproape toţi sunt de acord că „în viitor există posibilitatea ca adversarii să exploateze instrumentele şi tehnicile revoluţiei

---

87 Adam Herbert, „Air Force Officiai Calls Reduced Cycle Times Key To Info Superiority", Inside the Air Force, 21.06.1999. Potrivit articolului, Donahue (directorul comunicaţiilor şi informaţiilor aviaţiei militare americane) a numit forţa aliată „epoca ciber-războiului" din Cauza încercărilor sârbilor de a ataca sistemele informaţionale americane. ,*Din fericicre, acestea au fost la fel de eficiente ca şi apărarea lor aeriană, a glumit el".

88 Defensive Science Board, Task Force on Information Warfare-Dcfense, îl. 1996. Duane Andrews, preşedinte, apreciază că o dereglare majoră strategică e de Joasă intensitate" până în 2005.

89 Ibid.

informaţionale, pentru a ţine piept riscului (nu pentru a distruge, ci pentru a dezbina pe scară largă sectoarele naţionale strategice, cum ar fi diferite elemente ale infrastructurii naţionale: energia, telecomunicaţiile, transportul şi finanţele”[90].

Ar fi un act de iresponsabilitate să se ignore riscurile unor astfel de atacuri, considerându-le ca fiind imposibile. Ar trebui sa luăm în considerare ameninţările şi riscurile pentru a determina formele pregătirii şi răspunsului nostru.

Analiştii de la RAND văd două ameninţări la adresa SUA:

1. Ameninţare la adresa securităţii economice naţionale. Elementele infrastructurii naţionale pot ti supuse unor dezbinări produse de un atac care are succes. Acestea pot avea efecte strategice, printre altele, pierderea încrederii populaţiei în puterea de realizare a serviciilor infrastructurilor atacate.

2. Ameninţare la adresa strategiei militare naţionale. Există posibilitatea ca un adversar regional să utilizeze ameninţări sau atacuri tipice războiului informaţional strategic, pentru a deteriora sau a dezbina planurile americane dintr-o anumită zonă de criză.

Economiile sunt tot mai dependente de infrastructura informaţională. Orice afectează deliberat, într-un mod răuvoitor, capacităţile acelei infrastructuri poate fi numit atac. Dacă exist îi instrumente informaţionale de distrugere sau de dezbinare care să afecteze tranzacţiile financiare, băncile, serviciile de investiţii on-line, generatoarele de energie sau de distribuţie, telefoanele sau centrele de distribuire a informaţiilor, serviciile de urgenţă, etc., atunci, cel mai bun moment pentru un atacator de a face un test a fost perioada manifestărilor problemei Y2K.Problema Y2K este tratată aici ca un exemplu, ca posibilitate, chiar dacă ea pe moment s-a dovedit o alarmă falsă

90 „Executive Summary", Strategic Information Warfare Rising, ÏMR-964.0SD9V

Dacă SUA sau o alta ţară sunt ţintele unui viitor război informaţional strategic, atunci este probabil ca statele mici sau municipalităţile unui stat să devină ţinte ale testelor pentru atacuri le de tip Y2K. Oraşele din Europa de Est, din Orientul Mijlociu, din Asia de Sud, din America de Sud pot fi printre adversarii pe can trebuie să-i considerăm serioşi. Analizele de ţinte vor arăta entităt i particulare din cadrul statului candidat care sunt, în mod special vulnerabile (probabil o bancă sau o companie de telecomunicaţii)[91]. Cyber-atacurile ar prezenta un teribil avantaj: datele.

Un atacator va învăţa multe despre modul în care statele răspund în faţa unor inexplicabile probleme la nivelul infrastructurilor critice. Cum încearcă un stat să-şi protejeze sistemele fizice sau virtuale esenţiale pentru astfel de operaţii? Cum afectează atacurile asupra unor state mici economia interconectată? Ce puteri separate şi ce legături există între forţele armate şi autorităţile civile? Dar între guvern şi actorii comerciali? Ce pare să meargă bine şi ce nu? Ce sisteme sau elemente de infrastructură ne creează probleme mai mari? Cât de mult durează remedierea şi care sunt impedimentele unei remedieri rapide? Încrederea populaţiei este afectată?

Încă gândim proiectarea puterii în termeni de instrumente fizice şi încă gândim interzicerea accesului ca instrument de negare a abilităţii de mişcare a masei. „Accesul" poate fi abilitatea de a se apropia de un loc fizic sau de a introduce un grup acolo, dar accesul fizic este doar o *formă* a accesului. Există „locuri" electronice. Există elemente de acces pe piaţă.

Există un acces la realitate şi adevăr. În epoca informaţională, instrumentele puterii se schimba [92]. Cunoaşterea devine tot mai importantă, utilizarea ei conduce la acumularea bogăţiei şi violenţa e transformată

91 Jube Shiver, „Phone Firms may have a few Y2K Hang-Ups", Los Angeles Times, 24.05.1999.

92 Alvin şi Heidi Toffler, Powershift: Knowledget Wealth und Violence at the Edge ofthell Century, Bantam Books, NY, 1990.

prin luarea unui avantaj asupra ei. În secolul următor „accesul interzis” va fi prezent sub multe forme: incapacitatea de a introduce marfa, incapacitatea de a o susţine, incapacitatea de a participa pe o piaţă, şi de a cunoaşte adevărul. Însă unele din aceste fapte nu vor constitui un „acces interzis” prin ele însele.

Statele percep taxe pentru a împiedica un alt stat să-şi vândă mai ieftin produsele pe piaţa sa. Războiul comercial este în plină desfăşurare. Ministerul indian al Comerţului a declarat că „lipsa capacităţilor comerţului în ţara sa poate deveni o barieră a comerţului non-tarifar, împotriva exporturilor indiene într-o lume mai bună”96. Instrumentele non-violente pentru negarea accesului abundă deja şi războiul informaţional le va face pe toate mai subtile şi mai elegante. Scopurile războiului informaţional sunt cunoaşterea sistemelor adversarului şi exploatarea în propriul avantaj a slăbiciunii adversarului.

Imaginaţi-vă impactul interzicerii accesului unei pieţe. Un anume întreprinzător încearcă să stăpânească o piaţă, să-şi păstreze partea sau să capteze elementele critice, totul în scopul împiedicării accesului la această piaţă, sau ridicând costurile de intrare pentru noii competitori. În acest sens, multe companii aeriene de telefoane sau de alte utilităţi, au fost acuzate că pun în aplicare strategii de împiedicare a accesului şi a competiţiei.

Nu ar trebui să fim surprinşi că indivizi (sau state care îi sponsorizează), sindicate criminale, oameni de afaceri încearcă să împiedice accesul altora la propria afacere. Ceea ce surprinde este faptul că legea şi posesia unei afaceri legale poate preveni accesul. Da, anumite state puternice cred că pot lupta, în felul lor, împotriva acestor lucruri. Însă repertoriul global a instrumentelor de împiedicare a accesului continuă să crească şi multe au implicaţii în domeniul securităţii naţionale.

Cea mai bună utilizare a strategiilor de împiedicare a accesului este împiedicarea accesului la adevăr „. „Negarea şi decepţia” văzute în această lumină sunt

instrumente de împiedicare a accesului perfect, pentru că împiedică accesul la adevăr. Chiar dacă sunt utilizate pentru a proteja spaţiul lor privat, indivizii, grupurile sau statele pot împiedica accesul la cunoaştere şi sa mascheze semnificaţia lucrurilor şi acţiunilor observate. Acestea nu sunt în mod necesar acte de război.

Uitându-ne pe lista de mai jos, putem observa că puţine din elementele prezentate nu au participat la crearea cursului natural al lucrurilor. E puţin probabil că o proiectare sau o desfăşurare de sisteme ar putea avea loc efectiv, dacă s-ar confrunta cu aceste elemente în mod simultan.

Manifeste;

Distrugerea sau blocarea serviciului telefonic;

Bruierea undelor radio sau a celularelor;

Închiderea centrului de îngrijire a copiilor;

Răspândirea ştirii că Ebola sau E-coli se află în apă;

Activarea bombelor logistice;

Cauzarea unei bruieri a traficului prin dirijarea eronată a avioanelor sau altor vehicule publice;

Bruierea recepţiei TV;

Dezactivarea celularelor;

Încă o dată, o ocazie excelentă pentru a testa aceste efecte, a fost momentul creat de confuzia problemei Y2K. Nu sugerez că cineva face acest lucru, ci mai degrabă că cineva o va face.

Fără a trezi toţi dragonii teoriilor războiului rece trebuie să acceptăm că posedăm doctrine de utilizare a instrumentelor ostile cu intenţii ostile înainte ca formele familiare de ostilitate să erupă. Ostilitatea reprezintă utilizarea instrumentelor în scopul de a subjuga voinţa adversarului. Adversarul e subjugat atunci când pare a se purta ca agresor sau ca parte care se apără, în acelaşi mod în care noi intenţionăm să-l facem să se poarte 10°.

Şi această modificare de comportament poate să-şi aducă aportul înainte ca tradiţionalele (vechile) concepte ale operaţiilor de luptă să fie luate. Nu este vorba mai mult de „război”, decât de „pace”, pentru că războiul este doar

o parte a provocării asigurării securităţii în secolul XXI. Alvin şi Heidi Toffler sugerează că „o revoluţie în modul de a duce războiul, cere o revoluţie în modul de a face pacea”.,Pacea” trebuie să includă măsuri de „antirăzboi” pentru că faţa cealaltă a războiului este „pacea”, aşa cum cealaltă parte a războiului este „anti-războiul”[93].

Competenţa în timp de pace şi anti-război îi vor diferenţia pe cei care conduc provocările securităţii în prima parte a secolului XXI. Toffler observa faptul potrivit căruia „cunoştinţele reprezintă ceea ce anti-războiul va fi mâine” De aceea, e nevoie să se „accelereze colectarea, organizarea şi gestionarea noilor cunoştinţe, canalizându-le spre calea căutării păcii[94].

Un element important al noii cunoaşteri de care avem nevoie este cunoaşterea modului în care se utilizează războiul informaţional, sau contra-informaţiile ofensive, pentru a înăbuşi voinţa ostilă. În acest scop, aş vrea să prezint câteva principii care ar trebui să ghideze democraţiile în căutarea şi utilizarea acestor noi cunoştinţe. Unele principii pot provoca dezbateri aprinse, totuşi, ţelul meu este să generez o nouă cunoaştere în căutarea capacităţilor efective de anti-război, pentru a prezerva pacea.

Aceste principii se referă la secret, modelare, integrare, la modul de a cădea de acord în declanşarea evenimentelor, la prevenire şi la escaladare.

Aşa cum este dificil într-o democraţie să dezvolţi în secret noi arme şi capacităţi, orice cercetare şi experimentare a capacităţilor de contra-informaţii ofensive, trebuie să beneficieze de măsuri de restricţie drastice şi să fie bine compartimentate. Anumite capacităţi naţionale se cuvine să nu fie partajate cu aliaţii din cel puţin patru motive.

În primul rând, alianţele din următoarele decenii pol li vremelnice şi deci, instabile. Un aliat, la un anumit moment se poate afla de cealaltă parte. Capacitatea de a

93 Alvin şi Heidi Toffler, War and Anti-War.

94 Alvin şi Heidi Toffler, War and Anti-Warf p. 241.

surprinde poale dispărea dacă unul dintre foştii amici cunoaşte capacităţile acestuia. În al doilea rând, noile cunoştinţe de orice fel sunt proprietăţi intelectuale care pot fi evaluate.

A plăti nota pentru dezvoltarea unei noi proprietăţi intelectuale şi apoi a capitula nu este, în mod tradiţional, o afacere bună sau cel puţin, nu este o afacere bună de securitate naţională. De exemplu, să dezvolţi un nou cifru sau un nou cod pentru a proteja informaţia sau să dezvolţi noi capacităţi de spargere a codurilor pentru ca apoi să renunţi. În al treilea rând, există o legătură între orice nouă capacitate informaţională şi avantajele economice pe care aceasta le poate asigura posesorilor săi. De aceea, armele informaţionale, faţă de armele atomice, pot avea componente de mare utilitate pentru a realiza produse şi activităţi care nu au legătură cu sfera războiului. În al patrulea rând, nu ar fi inteligent să presupunem că celelalte state sau grupuri nu-şi dezvoltă în secret, capacităţi de război al cunoaşterii.

Pe de altă parte, a partaja anumite vulnerabilităţi şi tehnici de exploatare ofensive poate avea o considerabilă recompensă atât pe termen scurt cât şi pe termen lung. În primul rând, ar fi naiv să credem că cei care sunt angrenaţi în acest joc nu vor coopera pentru a acoperi largul spectru de atacuri care pot fi uşor dezvoltate de jucători de talie mult mai mică, dar dispersaţi în spaţiu.

O protecţie individuală a marilor jucători ar cere o multiplicare a eforturilor şi o dezvoltare a marilor resurse (dar totuşi finite) pentru a sprijini şi a conferi forţa unor mari organizaţii până la unele mai mici, mult mai concentrate asupra apărării şi agresiunilor -din sfera ciberspaţiului.

În al doilea rând, introducerea ameninţărilor adesea măreşte stabilitatea şi securitatea, prin stimularea dezvoltării şi desfăşurării măsurilor de protecţie, a celor motivaţi să-şi protejeze propriile sisteme. Cineva ar numi această tactică un „prezumtiv auto-atac”[95].

95 Richard Szafranski, « Awareness, Adritness, Audacy », o

Nu în ultimul rând, şi poate cel mai important, cel mai bun argument pentru partajarea cunoştinţelor ar fi că un astfel de lucru ar fi amplificat de efectele reţelei, un fenomen care a ajutat la crearea „exploziei cunoaşterii”, conduse de tehnologiile de comunicaţie. Deşi un asemenea schimb ar cere părţilor o siguranţă în privinţa obiectivelor comune pe termen lung, cea mai bună strategie ar fi să se echilibreze avantajul secretului cu beneficiile unor schimburi de cunoştinţe [96].

Unii ar putea argumenta că o atitudine secretoasă poate conduce la o spargere a alianţelor sau la atacuri informaţionale duse la întâmplare. Le voi răspunde că poate lumea deja este aşa. Competiţia la nivelul calculatoarelor, al aplicaţiilor software şi al telecomunicaţiilor creşte deja într-un ritm alert de cele două părţi ale Atlanticului. Fiecare companie sau naţiune speră să fie cu un pas înaintea celorlalte, pentru bogăţia propriilor acţionari. Ne aflăm deja aici.

Admit faptul că armele informaţionale sunt o nouă categorie de arme, dar cu greu fac distincţia între softul de anti-virus din zilele noastre şi armura folosită pe vremuri. Pentru a realiza o activitate de contra-informaţie defensivă trebuie bine cunoscuta capacităţile cerute pentru o activitate eficientă de contra-informaţic ofensivă.

Alianţele dintre state sunt puţin diferite de parteneriatele din afaceri. Statele au întotdeauna dreptul şi obligaţia de a abroga chiar şi cele mai solemne tratate în interes naţional. Încheierea unui parteneriat în afaceri păstrează aceleaşi prerogative. Ar li naiv să se creadă că alianţele sunt construite pe altceva decât interesele fiecărui stat membru.

Statele mai mici decât SUA vor protesta, bineînţeles, împotriva realizării în secret şi a nepartajării capacităţilor

---

Introducere la « Mastery of Information: Technology and Operaţional poncepts Circa 2030 » simpozionul Joint Expérimentation Futures ţWorkshop, 04.05.1998

96J 04 Brian Witten a numit acest lucru « Efectul de reţea al cunoştinţelor ».

naţionale americane (inclusiv ale războiului informaţional) ca fiind o nouă manifestare de, imperialism sau de izolaţionism. Însă SUA trebuie să se obişnuiască cu astfel de plângeri.

Secretul ne va expune pe toţi la o creştere întâmplătoare şi la o destabilizare a atacurilor inlormaţionale? Ar trebui să-i întrebam pe hackeri şi crackeri despre acest lucru. Instrumentele antidot dezvoltate în secret de state ar putea de fapt să mărească stabilitatea şi să evite atacurile întâmplătoare. Un hacker care simte greutatea puterii unui stat sau capacităţile contrainformaţiilor ofensive s-ar gândi de două ori înainte de a acţiona.

Netul şi Web-ul sunt noţiuni comune şi orice stat ar trebui să se simtă liber să acţioneze împotriva celor care nu au, o purtare corespunzătoare. Statele se vor comporta moderat, cred, cel puţin pentru că există o lipsă de tragere de inimă în a expune public existenţa armelor informaţionale din arsenalul lor. Păstrarea secretului este baza accelerării colectării, organizării şi generării acestor noi cunoştinţe. Şi păstrarea secretului este cheia pentru canalizarea acestor noi cunoştinţe spre căutarea mijloacelor de anti-război. Dar păstrarea secretului nu e o măsură suficientă.

MODELAREA va fi un pas esenţial în acest proces – dezvoltarea unei metode de abordare ştiinţifică pentru provocarea asigurării informaţionale. Comportamentul componentelor şi al sistemelor trebuie modelat (sistemele de stocare, comportamentul uman, erorile de sistem). Toate aceste modele trebuie să poată lucra împreună pentru a modela întregul sistem informaţional şi a cuantifica interdependenţele modelelor separate. Modelul dezvoltat trebuie să ţină seama de lucrările din trecut şi să dezvolte cercetarea, inclusiv modelarea dinamică şi sistemele bazate pe agenţi[97].

---

97 Michael Skroch, «Development of a Science-Based Approach for Information Assurance». Defense Advanced Research Projects Agency, Information Systems Office, 10.05.1999.

Astăzi înţelegem mai puţin decât avem nevoie să înţelegem să ne apărăm împotriva atacurilor şi să facem funcţional războiul informaţional şi ciber-războiul, pentru a aduce contribuţii semnificative războiului, anti-războiului şi păcii.

INTEGRAREA O dată ce putem modela operaţiile informaţionale trebuie să găsim căile eficiente de a integra capacităţile de război informaţional în diplomaţie, anti-război şi război. Cineva observa odată că diplomaţia este arta de a spune „frumos căţeluş, în timp ce ne uităm după un baston puternic”

Informaţia este cheia cunoaşterii căţelului care mârâie, a motivului mârâitului, a ceea ce îl sperie, a dimensiunii pe care o poate lua bastonul şi când şi unde poate fi „aplicat”. A aplica bastonul care trebuie căţelului este un lucru dificil, dar pentru a face acest lucru „cineva” trebuie să fie responsabil pentru integrare.

Poate cea mai bună integrare se face integrând substraturile diferitelor capacităţi. De exemplu, responsabilitatea privind masmedia trebuie acordată unui grup, iar comanda şi controlul reţelelor de calculatoare unui alt grup. Integrarea închide orice legătură existentă între forţele terestre, spaţiale şi aeriene, la fel de bine ca şi cele existente între afacerile externe, apărare, comerţ, etc.

La urma urmei, integrarea şi autoritatea trebuie să se găsească la şeful statului şi la comandantul tuturor categoriilor de forţe armate. Cu cât sunt mai repede înţelese capacităţile războiului informaţional ale unui stat, cu atât mai repede e nevoie de control şi execuţie centralizat! Probabil, paradigma controlului centralizai şi al execuţiei descentralizate se va transforma într-o autoritate centralizată a execuţiei şi a controlului descentralizat al instrumentelor.

Există astăzi asemenea agenţii de integrare? Nu ştim precis. Disputele recente nu au adus probe evidenfe ale eficienţei sau ineficienţei aplicaţiilor războiului informaţional. Genocidul pare să fi fost tolerat în Rwanda şi Iugoslavia, cu excepţia loviturilor împotriva trupelor

sârbeşti şi a capacităţilor de control ale forţelor paramilitare UCK albaneze. De asemenea, constatăm că embar goul informaţional rămâne fizic şi electronic şi impermeabil.

Scopul capacităţilor de integrare a operaţiilor informaţiona le este de a face posibil anti-războiul. Anti-războiul, se opune activ izbucnirii războiului şi necesită o mare atenţie acordată eveni mentelor trecute care au erupt în violenţă pâna la urmă. Integrare; operaţiilor informaţionale şi capacitatea de a conduce operaţii secrete, vor permite guvernelor să acţioneze repede şi tară a fi observate la cea mai mică comportare anormală. Un lucru nu trebuie să fie secret: categoriile comportării necorespunzătoare care cer un răspuns adecvat.

A CĂDEA DE ACORD ÎN DECLANŞAREA EVENIMENTELOR

Al doilea război mondial a fost un parametru al conduitei inadecvate, astăzi statele sunt mai permisive în privinţa unei proaste comportări a unui stat. Statul X îşi poate construi economia de export pe creşterea opiumului sau folosind abuziv copiii. Statul Y poate fi cel mai marc exportator de marijuana. Statul Z poate închide toţi practicanţii unui anumit grup etnic sau religios. Iar statul T poate reţine toţi teroriştii ceruţi de statele X, Y, Z. Respectul nostru pentru lege dus la extrem ne obligă să negociem cu teroriştii, criminalii de război, până când procesul se consumă.

Se poate observa că standardele noastre de moralitate şi legalitate nu pot fi făcute universale prin războaie violente, duse în afara limitelor noastre teritoriale. Totuşi, nu pot crede că războiul informaţional nu poate constitui un bun antidot pentru anumite forme ale unui comportament inadecvat, care nu se poate ridica uşor la nivelul declaraţiei de „război”.

Cu alte cuvinte, există evenimente a căror declanşare statele o pot recunoaşte ca indezirabilă sau în condiţii rele. Acestea pot fi uşor recunoscute în articolele care susţin motivaţia existenţei ONU. La fel ca embargourile,

operaţiile informaţionale pot asigura instrumente eficiente la constrângerile non-letale. Aparent ne lipseşte capacitatea şi curajul de a utiliza operaţiile informaţionale în situaţiile în care comportarea rău-voitoare necesită a fi pedepsită.

Păstrarea secretului va permite dezvoltarea capacităţilor, iar integrarea va da capacitate, însă curajul este o chestiune a fiecărei evaluări de risc şi a consecinţelor asupra fiecărui stat. Statele puternice sunt mai tolerante la riscuri decât cele slabe. De ce statele puternice nu s-ar pregăti să dea prioritate operaţiilor informaţionale?

PREVENIREA Aceasta este un instrument care cere contact fizic cu subiectul. David Ronfeldt, un strălucit cercetător de la RAND sugerează că democraţiile de tip „NET" se vor confrunta pe viitor cu „un nou model de conflict de joasă-intensitate, dar de un mare nivel social", foarte atrăgător pentru un lider care are trăsături psihologice nesănătoase şi „ale cărui ţeluri vor fi de a opera încet şi acoperit pentru a-şi slabi adversarii". Identificarea din timp a unor asemenea caractere ar fi folositor.

În tirnp ce angajamentele fizice atrag atenţia şi presupun riscul pierderilor de vieţi omeneşti, anumite operaţii de război informaţional nu comportă aceleaşi riscuri. De aceea, ne putem aştepta ca acele capacităţi de război informaţional create în secret şi integrate atacurilor non-militare şi non-tradiţionale, ca şi capacităţile de luptă tradiţionale să fie utilizate la fel de repede pe cât se declanşează evenimentele.

Forţele de atac nu vor cere permisiunea nimănui, cu excepţia şefului de stat, prietenii şi aliaţii nu vor fi avertizaţi, şi responsabilitatea nu va fi acceptată. Acest lucru va necesita o abordare a relaţiei civili-militari diferită. O astfel de necesitate va schimba relaţiile dintre luptători şi cei care nu luptă, dintre autoritatea civilă şi cea militară, şi, bineînţeles, vom numi în continuare statele noastre „democraţii".

Pentru aceste motive, dar şi pentru multe altele, aşteptăm noi concepte de operaţii informaţionale. În viitor, statele ar putea cere utilizatorilor de Internet să-şi imunizeze sistemele împotriva viruşilor distrugători. Pentru a asigura atât bunăvoinţa cât şi disponibilitatea, guvernul ar putea periodic să elibereze viruşi în sistemele sale, la partenerii săi şi inevitabil la noi.

Prevenirea ar putea deveni astfel o normă. Nu există încă o armă creată, pe care umanitatea să nu o fi folosit. Trebuie să credem că nu există nicio nouă armă, fapt care să reiasă din doctrina militară existentă în prezent şi din aceste discuţii despre războiul informaţional?

ESCALADAREA Toffler se întreba „dacă un adversar utilizează instrumente intangibile pentru a distruge sau provoca pagube unei anumite reţele de calculatoare ale unui oraş, inclusiv ale poliţiei, ale autorităţilor aeroportuare, a sistemelor electrice, bancare, etc.. Chiar dacă se presupune că se identifică sursa atacului, situaţia cere o intervenţie militară? A cui va fi responsabilitatea de a răspunde şi cum se va face acest lucru? Şi ce s-ar întâmpla dacă dezordinea provocată în oraş ar fi televizată în Mexic arătându-se imagini false despre măsurile brutale luate de poliţie împotriva sudamericanilor din L.A.? Dacă ar exista un război informaţional dus din interiorul şi din exteriorul SUA, măsurile de răspuns ar fi responsabilitatea FBI sau a militarilor?[98].

Nu există răspunsuri simple la aceste întrebări. Ştim că războiul informaţional urmăreşte modelarea comportamentului uman, în funcţie de scopurile sale. Ne putem închipui că panoplia armelor următoarei generaţii de război informaţional va include instrumente create pentru a afecta creierul uman: sunete, mirosuri, gusturi, imagini, senzaţii tactile. Ar putea include chiar şi droguri sau feromoni.

În acest caz, care nivel al atacului este just şi proporţionat şi care este neaşteptat, disproporţionat sau injust? Există vreun nivel al răspunsului just şi

98 Alvin Toffler, „Foreward", In Athena ' s Camp, p. 18.

proporţionat fără a cunoaşte bine statul sau grupul atacat?

Armele informaţionale sunt noi, şterg distincţia dintre luptători şi cei care nu luptă. Putem să ne punem aceleaşi întrebări ca în cazul forţelor nucleare? Ar împiedica statele războiul informaţional? Cum? În acelaşi mod prin care cursa înarmării nucleare a fost stopată: prin atingerea unei capacităţi suficiente pentru a nimici milioane de oameni? Sau ar trebui să creăm propriile noastre forţe informaţionale pentru răspunsuri flexibile sau selective? Ar fi înţelept să avem anumite opţiuni de răspunsuri „limitate" de război informaţional, dar să ţinem în rezervă altele „nelimitate"? Ar opta statele pentru o „asigurare de distrugere informaţională mutuală"? Am fi pregătiţi să tergiversăm un război informaţional?

Noţiunea probabilităţii erorii circulare va deveni instrumentul de calculat al probabilităţii erorii prin statisticile tehnice ale lanţului Markhov în războiul informaţional?

Care sunt canoanele pagubelor epistemologice acceptate sau a probabilităţii pagubelor? Ce este o „pagubă informaţională colaterală" şi cum va fi controlată? Există o apărare civilă împotriva nivelului strategic de război informaţional?

Cine va asigura managementul războiului informaţional şi cum? Va susţine cineva „îngheţarea armelor informaţionale" sau o „zonă liberă" a acestora? Există multe alte întrebări referitoare la implicaţiile războiului informaţional.

Dacă războiul informaţional nu este un lucru serios, cum se explică existenţa în SUA a unor entităţi ca „Centrul armatei privind activităţile de război informaţional", „Centrul de război informaţional al forţelor aeriene", „Activitatea navală submarină de război informaţional", „Centrul flotei de război informaţional"?

CONCLUZII

Războiul informaţional reprezintă utilizarea cunoştinţelor pentru a contopi cunoaşterea cu acţiunea efectivă. Tehnologia se află deja aici, însă tehnicile

aşteaptă încă teste şi procese. Cred că vom asista la o serie de teste şi procese de tipul manifestărilor problemei Y2K.. Pentru a ne proteja şi a proteja sistemele informaţionale trebuie să facem mari progrese în modelarea, integrarea, securitatea acordului în declanşarea evenimentelor, înţelegerea prevenirii şi a escalădării. Multe din acestea trebuie să se desfăşoare în secret. Ceea ce va fi vizibil va fi nivelul reuşitei noastre. Cunoaşterea, după cum spunea Toffler, este lucrul despre care va fi vorba în războaiele şi antirăzboaiele de mâine.

REVOLUŢIA INFORMAŢIONALĂ

PATRICK TYRRELL*

Acest material examinează natura informaţiei şi observă cum aceasta se transformă, în epoca „post revoluţiei informaţionale”. A schimbat acest lucru modul în care o foloseam? A modificat maniera în care noi, ca oameni, răspundem la ea?

Voi încerca sa examinez, câteva potenţiale ameninţări şi modul în care integritatea informaţiei poate fi mai bine păstrată. Voi ridica o serie de probleme importante, dar la care nu există încă răspunsuri: cui revine responsabilitatea pentru păstrarea informaţiei?

Cum poate un stat să-şi exerseze suveranitatea asupra informaţiei şi fluxului informaţional? Cum pot fi controlate reţelele globale şi ce ameninţări la adresa integrităţii informaţiei naţionale pot fi identificate? Acestea sunt câteva probleme care aşteapta încă răspuns, lucru care nu ne va impiedica să ne aventurăm pe tărâmul informaţiei.

„De *abia acum începem să realizăm dimensiunea şi profunzimea schimbărilor în condiţiile vieţii umane, proces care continuă să se desfăşoare. Noţiunea de distanţă se modifică, puterea fizică disponibilă a devenit foarte mare, suveranitatea statelor imposibilă*

H.G. Wells[99]

„Electronul după părerea mea, este precizia din

99 H,G Wells, A Short History of the World, London Penguin, 1936.

urmă carc ghidează în *uniţia*

John Deutch Director CIA în”

Pe măsură ce ne apropiem de sfârşitul secolului XX, jurnalişti, scriitori, oameni de ştiinţă şi comentatori s-au întrecul în a atinge un anumit grad de imortalitate cu ajutorul „biţilor de sunet”. Un concept care s-a impus de la sine în conştiinţa publica este,/evoluţia informaţională”, având des o vagă înţelegere a ideilor implicate.

Un cuvânt care a pătruns în lexicul popular, ca rezultat al acestei revoluţii este „ciberspaţiul”, inventat de un scriitor de science-fiction american în anii 80, observând câţiva băieţi jucând jocuri pe calculator, foarte captivaţi de lumea virtuală.

Există un întreg comerţ cu cărţi, articole, reportaje sau discuţii asupra implicaţiilor revoluţiei informaţionale în fiecare aspect al efortului uman. Nu putem concepe viaţa modernă fără convenienţa, rapiditatea şi universalitatea sistemelor informaţionale de azi, de la modestul telefon la posibilitatea de a participa la discuţii în grup pe Internet, de la cartea de credit la manipularea pieţelor financiare, 24 de ore din 24.

Aceste exemple, ca multe altele, conduc la ideea că fluxul informaţional nu poate fi împiedicat, că informaţia recepţionată e corectă, şi nu coruptă, şi e cât se poate de clară. În multe cazuri, se va porni de la ideea că fluxul informaţional e privat şi ca informaţia e confidenţială între emiţător şi receptor.

Integritatea informaţiei a fost întotdeauna o problemă de interese critice, însă schimbările dramatice introduse de revoluţia informaţională au făcut mult mai dificil de urmărit traseul pe care îl urmează informaţia de la un punct la altul.

Tocmai această inabilitate de a identifica cu uşurinţă provenienţa informaţiei, la care se adaugă sistemele moderne care permit o interconectare globală, au permis dezvoltarea globală a crimei organizate, caracterizată ca fiind cea mai mare afacere, cu profituri estimate, în 1998, la un miliard de dolari. În domeniul militar, aceleaşi

condiţii au dat naştere conceptului de *război informaţional*, prin care un potenţial adversar poate încerca să exploateze vulnerabilităţile din cadrul sistemelor informaţionale naţionale ale unui stat.

Aş dori să examinez termenii care sunt des folosiţi pentru a descrie anumite concepte care modelează perspectiva modernă a informaţiei. Alvin şi Heidi Toffler includ în largul concept al cunoaşterii informaţiile, datele şi cultura. Schwartau consideră datele Ca fapte individuale sau statistice într-o formă necorelată, care, odată organizate, devin informaţii.

Transformarea informaţiei în cunoştinţe se realizează în momentul în care intervin intuiţia şi gândirea umană. Un academician francez, Philippe Baumards[100] merge mai departe şi argumentează că o societate fundamentată pe filosofia grecoromană, limitează bazele sale de cunoştinţe mai degrabă la „*cunoştinţe* obiectivedecât la cele incluzând perspective mai largi, cum ar fi „*cunoştinţele conjuncturale*". Baumard face astfel o distincţie între, *jn formare*" şi „*cunoaştere*".

Acesta consideră că multe organizaţii, mai ales cele care funcţionează în perioade de schimbări considerabile, cred că trebuie să utilizeze din ce în ce mai multe cunoştinţe şi acest lucru le forţează să proceseze tot mai multe informaţii. În opinia lui Baumard, organizaţiile şi indivizii care au succes acordă mai multă atenţie „simţului practic", decât colectării simple de informaţii.

Fukuyama examinează rolul erei informaţionale în erodarea ierarhiei şi autorităţii în societate şi accentuează rolul încrederii şi partajării normelor etice, care reprezintă fundamentul unei societăţi. O bună informaţie va spori abilitatea omenească de a raţiona.

Valoarea „*informării*"*este* similară filosofiei lui Sun Tzu care spunea că un lucru important este să distrugi strategia adversarului înainte ca acesta s-o pună în

---

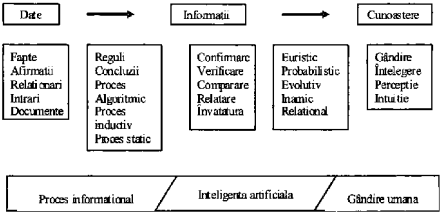
100 Ph. Baumard, From Info War to Knowledge Warfare: Preparing for the Paradigm Shift, Info War Con, Bruxelles, 05.1996.

practică. Acest lucru trebuie făcui într-o manieră neaşteptată, printr-o utilizare neconvenţională a „forţei divine” (*ch'i*).

Opusul lui *ch'i* este forţa comună (*cheng*). Pe câmpul de lupta, *cheng* e o forţa care doboară adversarul imediat, în timp ce *ch 'i* reprezintă manevra de flancare care distruge în mod fatal strategia inamică [101]. Acestea sunt şi ideile care stau în spatele conceptului lui Edward de Bono „*gândireaparalelă*”: „în gândirea paralelă se pune un mare accent pe concepte şi pe informaţie”[102].

De ce am fi interesaţi de aceste diferenţe şi cum ar putea ele să ne ajute să înţelegem problemele legate de integritatea informaţională? Există o tendinţă aparent naturală, în domeniul tehnologiei informaţionale, ca şi în cel al tehnologiei în general, care permite tehnologiei să conducă dezvoltarea sistemelor care privesc mai ales, necesităţile societăţii sau pe cele ale organizaţiilor. Înţelegerea aspectelor umane ale procesului decizional este importantă dacă dorim să ne oprim asupra zonelor în care integritatea poate fi vitală şi să identificăm domeniile în care o siguranţă a integrităţii e, cel puţin, la fel de importantă.

Doctrina militară de comandă-control (C2W) se axează pe ceea ce e nevoie pentru a influenţa comportamentul uman şi definiţiile includ utilizarea integrată a distrugerii fizice, a războiului electronic, a înşelătoriei, a operaţiilor psihologice şi a operaţiilor de securitate.



1011 J4 „Survey of Defense Tehnology", The Economist, 10.06.1995.

102 Edward de Bono, Parallel Thinking-From Socratic to de Bona Thinking, Viking,1994.

Figura 1: Spectrul cunoaşterii

Utilizarea unor astfel de tehnici poate afecta modul în care un decident va interpreta informaţia, structurându-se după tendinţa sa naturală de a gândi mai mult inductiv decât „lateral”. O astfel de viclenie de război posedă o bogată istorie, de la Calul troian la „Mary how never Was”.

Este interesant de urmărit munca pe care au depus-o experţii în sisteme [103], în care un atribut esenţial al acestor sisteme comparate cu programele convenţionale este natura euristică.

Este vorba de o revoluţie a cunoaşterii care scoate în evidenţă accentul pus pe fluxul informaţional şi accesibilitatea cunoştinţelor. Conceptul „capital intelectual” e din ce în ce mai acceptai ca noţiune în lumea comerţului, ca unul din cele mai importante bunuri ale unei companii.

Dezvoltarea unui astfel de bun este cheia succesului, după cum o poate certifica creşterea fenomenală a anumitor companii Internet, ca *Amazon*, *com*. Este interesant să privim *Spectrul cunoaşterii* din Fig. 1. Acesta ilustrează legăturile dintre un anumil număr de concepte şi procesele de control ale transformării datelor în informaţii, de virtuţile umane tradiţionale prin care informaţia devine cunoaştere.

Există şi patru stadii cheie ale ciclului de viaţă al informaţiei: crearea, culegerea, diseminarea şi utilizarea ei.

Figura 2: Ciclul de viaţă al în formaţiei

Aceste patru cicluri sunt distincte, deşi au multe caracteristici în comun. Dezvoltarea tehnologică din ultimii ani a afectat viteza şi volumul culegerii şi diseminării informaţiei. Pentru a fi eficaci.

trebuie să utilizăm mai bine informaţia şi să ne

103 Peppard, IT Strategy for Bussiness, Piunan Publishing 1993.

dezvoltăm abilitatea de a dirija acţiuni mai bune.

Informaţia a constituit întotdeauna un aspect important al societăţii umane. Capacitatea de a comunica idei şi concepte a fost considerată că fiind una din caracteristicile *homo sapiens*. Dezvoltarea mijloacelor de tipărire în Europa, datorită lui Gutenberg şi Caxton, în secolul al XV- lea, a avut o influenţă profundă asupra educaţiei şi a lărgirii fundamentului intelectual, prin asigurarea unor surse de cunoştinţe relativ ieftine şi consistente unei audienţe mult mai mari, decât până în acel moment. De abia în a doua jumătate a secolului XIX s-a produs un nou salt, care a contribuit la îmbunătăţirea mijloacelor de transfer ale cunoştinţelor.

Apariţia telefonului şi a tehnologiilor transmisiilor fără fir, a permis transmiterea instantanee a informaţiilor la distanţă. Totuşi, acest transfer de informaţii rămânea un proces linear şi transparent prin care datele erau evaluate, după care informaţiile analizate erau disponibile a fi transferate la utilizator, care putea astfel, să acţioneze în consecinţă. Receptorul poate, dacă e necesar, să urmărească o revizuire a drumului parcurs pentru a evalua validitatea informaţiei.

Aşa, de exemplu, dacă în bătălia de la Waterloo, Wellington ar fi dorit să-şi amendeze tacticile, ar fi scris noile sale ordine şi le-ar fi înmânat comandantului potrivit pentru a le pune în aplicare. Dacă corpul mesagerului ar fi fost descoperit mai târziu cu sacul gol s-ar fi ajuns la concluzia că informaţia din mesaj a ajuns în mâinile francezilor.

Dacă prima jumătate a secolului XX a fost martora unui anumit număr de îmbunătăţiri calitative a modului în care datele puteau fi transmise în lume, imperativele tehnologice ale celui de-al doilea război mondial au asigurat îndeplinirea viziunii lui Babbage: calculatorul şi prin urmare, revoluţia informaţională.

Ca multe dezvoltări tehnologice, de-a lungul istoriei, forţele care s-au aflat în spatele inovaţiilor acestei revoluţii au fost aproape exclusiv militare, reflectând priorităţile

celui de-al doilea război mondial şi pe cele ale războiului rece.

Marea schimbare a reprezentat-o faptul că factorii care determinau progresul acestor tehnologii se sprijineau mai puţin pe bugetele apărării sau pe alte resurse guvernamentale şi mai mult pe priorităţi comerciale, aplicări şi presiuni. Motivele acestei manevre sunt complexe, contribuind mult la stabilitatea şi prosperitatea de care s-a bucurat Vestul în perioada războiului rece, dar şi la abilitatea sferei comerciale de a dezvolta o piaţă globală şi competitivă.

Termenul „revoluţie" a fost utilizat, în ultimul timp, mai ales pentru a caracteriza dezvoltarea tehnologiei informaţionale din ultimul deceniu. Dacă acum 50 de ani calculatoarele tindeau să automatizeze activităţile umane pentru a obţine rapiditate şi precizie, funcţiile acestora putând fi înlocuite de procese manuale, în schimb, sistemele moderne sunt interconectate şi interdependente şi nu mai pot fi considerate sisteme manuale.

Ştiinta şi tehnologia ne promit că într-un viitor apropiat, sistemele de inteligenţă artificială vor realiza activităţi ce acum sunt îndeplinite de om. Doar un control uman limitat va fi necesar şi majoritatea operatorilor se vor mulţumi să răspundă doar la ceea ce le vor cere software-uri sofisticate.

Există deja un număr important de implicaţii perturbatoare datorate dependenţei de sisteme, mai ales la nivelul copiilor, care-şi pierd capacitatea instinctivă de înţelegere şi apreciere asupra problemelor matematice, când sunt prea preocupaţi de calculator. Aceştia aşteaptă informaţiile fără să le verifice validitatea. Şi trebuie să ţinem seama că aceşti copii vor fi managerii de mâine.

Într-un raport examinând doborârea avionului iranian Airbus 655 de către USS Vincennes, în 03.07.1988, Rochlin ' menţionează câteva pericole ale dezvoltării instrumentelor sotisticate, ale dispersării sistemelor centralizate de comandăcontrol, acestea devenind mai rigide şi tot mai saturate de informaţie şi responsabilităţi,

Iară a se înregistra vreo îmbunătăţire a capacităţilor umane de a controla asemenea concepte.

Ar fi greşit să ne concentrăm exclusiv asupra noilor tehnologii ale revoluţiei informaţionale. Tehnologia, chiar dacă este foarte sofisticată, reprezintă mai degrabă un instrument de manipulare a informaţiei, care să pună cap la cap, să stocheze, să sorteze, să rafineze şi să asambleze informaţiile pe care le cere utilizatorul. Calculatoarele moderne pot stoca informaţiile, le pot procesa şi le pot distribui apoi în moduri nemaiîntâlnite până acum, făcând posibile mari beneficii în domeniul afacerilor, dar sporind şi gradul şi oportunităţile pentru un management defectuos, prin pierdere, neglijare sau diseminare discriminatorie a informaţiei.

Informaţia, ca bun militar strategic, a fost întotdeauna recunoscută ca atare de către comandanţi, mai ales în ideea unei bune cunoaşteri a intenţiilor adversarului şi în acelaşi timp, a unei protecţii proprii a planurilor şi a stadiului operaţional. Făcând această informaţie disponibilă în domeniul militar, de la nivelurile strategice de comandă la comandanţi, apar o serie de probleme în privinţa încrederii acestora în integritatea, relevanţa şi validitatea informaţiei prezentate. Distrugerea Ambasadei chineze din Belgrad de avioanele NATO constituie un exemplu al pericolului pe care-l prezintă acceptarea informaţiilor fără a le verifica provenienţa.

Extinderea revoluţiei informaţionale la organizaţii, civile sau militare, nu a fost benefică tuturor. Strassman considera că nu există o legătură directă între beneficiile acţionarului şi costurile pe care le suportă o firmă pentru tehnologia informaţională. Această perspectivă este susţinută de un studiu al revistei *The Economist*care vorbeşte de introducerea electricităţii în industria americană la începutul secolului XX, când beneficiile financiare începeau să apără, odată cu orientarea managerilor spre noile tehnologii.

Natura operaţiilor militare şi expunerea lor la o radiografiere permanentă a mass-mediei, va constitui o

greutate în plus pe umerii decidenţilor militari, cu consecinţe dramatice, în caz de insucces. Pentru a descoperi nevoile informaţionale ale comandanţilor militari, este necesar să examinăm tipul activităţilor militare în care sunt angajaţi.

Există o diferenţă considerabilă între necesităţile informaţionale cerute de operaţiile de menţinere a păcii, de exemplu, şi cele cerute în timpul unui conflict major. Acest „spectru al conflictului" asigură un instrument analitic util şi ne poate permite, să distingem un anumit număr de legături comune.

Recentele operaţii din Kosovo, de exemplu, au scos în evidenţă cerinţele pentru o capacitate de mişcare dintr-o parte a acestui spectru în cealaltă. Actuala operaţie de menţinere a păcii poate degenera foarte repede într-un nou conflict.

O examinare fugară a sistemelor informaţionale moderne dezvăluie faptul că instituţia militară nu mai reprezintă motorul central al cercetării şi dezvoltării tehnologiei. În momentul de faţă domeniul economic iniţiază şi conduce cercetările şi dezvoltarea ei, într-o manieră nouă. Firmele comerciale îşi reconsideră sistemele informaţionale pe care le înlocuiesc la intervale regulate de timp. Necesităţile militare şi cele guvernamentale sunt stabilite mai degrabă pe zece ani şi nu patru sau cinci ani cum procedează societăţile comerciale.

În acelaşi timp, sistemele militare se interconectează tot mai mult cu cele din lumea civilă ceea ce ridică tot mai mult problema interoperabilităţii dintre aceste sisteme. Pe măsură ce presiunea asupra militarilor creşte în privinţa iniţiativelor de genul finanţării private, creării de agenţii şi pe măsură ce creşte şi nevoia unor legături mai strânse cu firmele civile, datorită dezvoltării şi supor tului lor, cresc şi riscurile aferente unei asemenea interdependente

Există un anumit număr de ameninţări pe care le putem identifica, la adresa integrităţii informaţiei.

Există trei parametri cheie pentru evaluarea naturii

ameninţărilor: identificarea autorului, a *modus operandi-ului* şi a motivului.

Una din caracteristicile ameninţărilor asupra informaţiilor digitale este dificultatea identificării autorului. Sunt mai multe cauze care ar putea conduce la lansarea unui atac informaţional:

Un hacker care consideră o anumită reţea o provocare;

Un angajat nemulţumit;

Un criminal profesionist care încearcă să spargă sistemul de securitate pentru a obţine un anumit profit;

O companie naţională sau multinaţională care încearcă să obţină avantaje comerciale în dauna competitorilor săi;

O organizaţie non-guvernamentală internaţională care doreşte să-şi pună în aplicare planurile;

Servicii secrete ostile, care încearcă să identifice şi să exploateze punctele de vulnerabilitate ale unei alte ţări, a infrastructurii sale militare şi comerciale;

Organizaţii teroriste care doresc să distrugă infrastructura socială, comercială sau militară a unui stat.

Modul de operare adoptat de autori variază, însă un instrument frecvent utilizat sunt viruşii. Dezvoltaţi de către un profesor în matematică de la Universitatea din Sofia, aceştia sunt acum parte integrantă a domeniului calculatoarelor. Viruşii continuă să afecteze lumea informaţională, după cum s-a văzut şi în prima parte a anului 1999 (Melissa, Cemobâl). Se estimează că aproape 200 de noi viruşi sunt creaţi lunar [104].

Motivul atacului poate determina nivelul ameninţării pentru © organizaţie şi identifica acţiunile necesare pentru a neutraliza Ameninţarea. Pentru a examina motivul, trebuie să ne uităm la tipul atacului. Pe lângă atacurile intenţionate, orice infrastructură informaţională va fi vulnerabilă la nenumărate evenimente, iar o protecţie faţă de acestea se poate realiza chiar în sistem. Aceste

104 Stoll Clifford, The Cuckoo 's Egg, London, Bodley Head, 1990.

evenimente includ dezastrele naturale.

O problemă mai serioasă este răspunsul dat la un act deliberat: acesta poate merge de la accesul neautorizat la furtul de informaţii, la distrugerea datelor, la inserarea de informaţii derutante în baza de date sau scoaterea din funcţiune a sistemului. Un astfel de exemplu este atacul asupra facilităţilor USAF de la Rome Air Development Center, din martie şi mai 1994 [105]. Acest atac a compromis câteva sisteme, prin folosirea unor tehnologii care detectează identitatea şi parola utilizatorilor.

Hackerul a utilizat mai multe site-uri localizate aparent în diferite ţări (din Europa, America de Sud şi Mexic) pentru a nu i se da de urmă. Când a fost în sfârşit prins de Scotland Yard, s-a constatat că acesta avea doar 16 ani şi că trăia la Londra.

Capacitatea de a ascunde sursa atacului este una dintre caracteristicile tehnologiilor moderne, o formă de *„opacitalc informaţională”* care are multe implicaţii. Dacă un stat sau o organizaţie doreşte să lanseze un atac împotriva altui stat sau organizaţie, acest lucru poate fi realizat prin intermediul unui al treilea stat sau organizaţie, dând impresia ţintei că a treia parti* este autorul real al atacului. Am aratat deja că împletirea şi interconectarea sistemelor şi un atac deliberat la adresa suportului infrastructurii, cum ar fi la nivelul legăturilor comunicaţiilor, la sistemele din afara organizaţiilor, la nivelul rapoartelor Reuters, a informaţiilor comerciale sau a rapoartelor pentru logistica militară realizate pentru furnizori, pot avea consecinţe serioase pentru organizaţie.

Graniţele care delimitează orice organizaţie nu mai sunt impenetrabile ci permeabile informaţiilor digitale. Acest lucru este luat în discuţie mai jos, punându-se accentul pe problema suveranităţii naţionale.

Orice strategie creată pentru a proteja informaţia strategica a unei organizaţii trebuie să examineze legăturile dintre propriii» sisteme informaţionale şi cele exterioare.

---

105 CSIS Report on Global Organised Crime.

Deşi identificarea unui atac serios este greu de realizat, doar câteva atacuri sunt recunoscute ca atare de către utilizatorii sistemelor. Preşedintele SUA a cerut elaborarea unui studiu privind „Infrastructura Naţională critică”, iar în Marea Britanie Home Secretary a devenit responsabil pentru protecţia comerţului electronic din UK [106].

Cum să protejăm sistemele militare sau civile când ele sunt interconectate cu altele? Pentru a putea evalua tipul necesar de protecţie, câteva tehnici de management al riscului vor trebui să fie dezvoltate urmărind:

Să identifice vulnerabilităţile informaţionale din interiorul sistemului şi între sisteme;

Să identifice potenţialele ameninţări;

Să clasifice ameninţările;

Să dezvolte strategii potrivite de recuperare.

Dezvoltarea strategiei potrivite de acoperire este un lucru foarte important. Din datele deţinute de Departamentul American al Apărării reiese că există un număr mare de încercări de spargere a sistemelor militare şi civile şi că acest număr este în creştere ca urmare a interconectării existente şi a creşterii gradului de sofisticare al instrumentelor utilizate de hackeri. Programul RI defensiv al SUA identifică trei faze de comportare: protecţie, detecţie ţi reacţie.

Acest lucru permite sistemelor să fie protejate într-un mod cât mai practic, în timp ce sunt activate pentru a detecta intruşii într-un cadru organizaţional de dorit, creat pentru a raporta spargerile şi pentru a reacţiona rapid, pentru a preveni viitoare atacuri, a ameliora pagubele şi a restaura serviciile cât mai repede. Această activitate se concentrează asupra sistemelor din cadrul unei organizaţii şi nu se interesează de vulnerabilităţile existente la nivelul sistemelor exterioare organizaţiei.

Bineînţeles că nu este doar foarte costisitor să protejezi toate sistemele, dar nici nu e practic şi, în consecinţă, în privinţa sistemelor care nu cer o securitate

106 Declaraţia din Parlament a Home Secretary, 25.01.1999.

sporită, politica instituţiei trebuie să se concentreze asupra elementelor „detectare” şi „reacţie”. Stabilirea siguranţei informaţionale potrivite are, deci, o importanţă majoră şi va cere pe viitor rutină şi o riguroasă „revizie informaţională”.

Acestea vor fi similare cu cele care se realizează în cadrul organizaţiei azi, pentru a monitoriza evaluările strategice, ca cele financiare şi de personal. Revizuirea va urmări a examina ce informaţie e cerută de utilizator, de unde vine informaţia şi cum e procesată.

Cine trebuie să fie responsabil de asigurarea securităţii informaţiei? Să fie vorba doar de o competenţă tehnică sau de o funcţie managerială? Consecinţele căderii unui sistem pot fi atât de grave încât să-i afecteze pe toţi membrii staff-ului unei organizaţii şi deci responsabilitatea asigurării integrităţii informaţiei le revine tuturor.

Managerii ar trebui să determine politica organizaţiei pentru bunurile informaţionale şi să identifice cum aceasta poate fi măsurată şi revăzută. Lista problemelor care trebuie luate în seamă cuprinde identificarea acelor bunuri, calitatea şi cantitatea informaţiei cerute şi protejarea informaţiei împotriva accesului neautorizat, de abuz sau de folosire greşită.

Organizaţiile trebuie să examineze problema interconectări i sistemelor şi potenţiala creştere a dependenţei organizaţiei de sistemele altei organizaţii. Un exemplu este cel al utilizării capacităţilor telefoniei comerciale pentru acoperirea nevoilor proprii unei organizaţii.

Deşi utilizarea serviciilor ar trebui să presupună şi asigurarea unor servicii acceptabile, vor exista tot mai multe motive pentru folosirea unei asemenea interconectivităţi în scopuri mai puţin onorabile. Acest lucru se întâmplă deja cu organizaţiile conectate la Internet.

Devine limpede că problema integrităţii informaţiei este una care afectează companiile, corporaţiile multinaţionale, guverne k şi, în cele din urmă, relaţiile

dintre state. Este instructiv să nc aplecăm asupra genezei conceptului război informaţional, asupra relaţiei dintre ethos-ul informaţiei militare şi elementele sale civile şi să examinăm implicaţiile asupra suveranităţii statelor-naţiune.

Este clar ce înseamnă un „act de război” în cazul unui atac convenţional, împotriva unui stat. Un astfel de atac va fi urmat de o declanşare a ostilităţilor, aşa cum s-a întâmplat, de exemplu, după ce forţele argentiniene au invadat insulele Falkland, în aprilie 1982. O definiţie asupra „războiului” a fost data de Malinowski (1968): „lupta armată între două unităţi politice independente, utilizând forţe militare, urmărind o politică naţională sau tribală[107]. Atacurile germane asupra Londrei în cel de-al doilea Război Mondial sunt acoperite de această definiţie. Aceste atacuri destinate distrugerii capacităţii Londrei de a funcţiona ca un centru financiar şi comercial, erau realizate de „forţe militare organizate”.

Însă la un atac electronic, considerat act de război se poate răspunde la fel, dacă autorii nu sunt state-naţiune, ci o instituţie multinaţională, de exemplu? Acesta devine o interogare intelectuală interesantă: dacă un stat nu poate spune ce e un război, sau să determine cine conduce un atac menit să provoace pagube, să distrugă importante bunuri naţionale, cum ar fi oraşul Londra, stabilitatea viitoare a statelor-naţiune ar putea fi în primejdie.

În acest caz, cine, în cadrul statului-naţiune trebuie să se ocupe de asigurarea unei apărări potrivite? Încă nu există o coerenţă la nivelul guvernului şi a lumii economice în privinţa abordării problemei atacurilor realizate prin intermediul sistemelor electronice.

Termenul de „război” este peiorativ şi aduce aminte de comentariul lui John Fowles [108]: „Bărbaţii iubesc războiul pentru că acesta le permite să pară serioşi. Pentru că este sigurul lucru de care femeile nu râd de ei”.

---

107 The Oxford Companion to Politics of the World, Oxford University Press, 1993.

108 John Fowles, The Magus, London Jonathan Cape, 1977.

S-au făcut progrese considerabile, în ultimii ani, despre cum războiul informaţional poate constitui o nouă unealtă capabilă sii atace societatea. Nu cred că e vorba de o nouă problemă, ci mai degrabă că a devenit mai insidios prin capacitatea de a culegi* mari cantităţi de informaţie şi de a le disemina la nivel global. Discuţiile asupra războiului cibernetic şi a războiului informaţional se poartă în jurul ideii folosirii unor astfel de atacuri împotriva unui stat-naţiune, ca alternativă la atacurile convenţionale.

Acestea includ acele activităţi care nu corespund, în mod normal, normelor militare, dar care reflectă creşterea dependenţei activităţilor guvernamentale şi comerciale de diferite sisteme, vitale pentru funcţionarea operaţiilor militare modeme. Practic, de la un calculator anonim se pot cauza pagube considerabile Iu nivel politic, social, financiar, etc.

Sintagmele *Infrastructură Naţională Informaţională* (INI) şi *Infrastructură Informaţională Globală* (IIG) sunt destul de populare în SUA şi reflectă natura organică şi dinamică a reţelelor informaţionale care s-au dezvoltat în sprijinul nivelelor de interconectivitate, dependenţă şi integrare cerute. În ciuda numelor, nici INI şi nici IIG nu există că sisteme integrate. Nu sunt proprietatea nici unei agenţii sau companii, guvernul exercita o mică influenţă în procesul general de dezvoltare şi sunt animale de cererile consumatorilor.

Aceste infrastructuri constau într-o multitudine de sisteme, de legături de comunicaţie şi facilităţi. Există un flux continuu de informaţie la nivel global, volumul acestuia crescând exponenţial pe măsură ce „infrastructura globală” continuă să se dezvolte. Vulnerabilităţile unor astfel de sisteme sunt numeroase, greu de identificat şi nu pot fi evaluate corespunzător, datorită ritmului dinamic al schimbării şi incapacităţii de a defini sistemul general.

În lumea occidentală, Londra îşi menţine rolul de actor majoi în activităţile financiare şi comerciale.

Fluxurile informaţionale sunt cheia succeselor sale: pieţele financiare sunt acum contrôlait prin operaţii electronice globale realizate în timp real, care se ridica la un cost de trei milioane £ pe an. Pagubele aduse companiei „The Baltic Exchange" datorită bombelor IRA, au produs disfuncţii importante în activităţile comerciale ale Marii Britanii.

Activităţile unui singur comerciant din Singapore duce la decesul uneia dintre cele mai prestigioase bănci engleze, prin preluarea sa de către o bancă daneză. Beneficiile Marii Britanii în urma unor astfel de activităţi în Londra sunt considerabile şi se reflectă în balanţa de plăţi naţională. Este cert că un anumit număr de ţări, instituţii şi corporaţii ar dori să vadă schimbat acest statut. E posibil ca pe viitor unii să se pregătească să precipite o astfel de schimbare, prin activităţi care să afecteze infrastructura informaţională a oraşului.

Blackstone a definit suveranitatea ca fiind „regula de acţiune prescrisă sau dictată care trebuie ascultată". Suveranitatea este un concept central a definiţiei statului-naţiune. Din punct de vedere istoric, era considerată un concept secularizant, care reflectă declinul universal al autorităţii religioase, care încuraja ideea supremaţiei statului asupra teritoriului său [109].

Pentru că nu există un super-stat care să controleze statul, fiecare stat e „suveran" în cadrul societăţii internaţionale. La sfârşitul primului război mondial, preşedintele american W. Wilson a propus 14 puncte care reprezentau o încercare de îngrădire a suveranităţii naţionale[110]. Acest proces a fost continuat de ONU care, deşi este o organizaţie care asociază state suverane, îşi rezervă dreptul să intervină pentru implementarea măsurilor care să asigure pacea [111]. Acest lucru este

109 A se vedea Oxford Companion to Politics of the World, Oxford University Press, 1993.

110 Hugh Brogan, History of the United States of America, Longman, London 1991.

111J 27 Peter Calvocoressi, World Politics since 1945, Longman,

evident în acţiunile întreprinse în Irak după războiul din Golf, ca şi în cele din Iugoslavia, în care ONU şi NA TO au intervenit într-o problema naţională.

În Europa, dezvoltarea Uniunii Europene a necesitat un transfer de suveranitate către Bruxelles, în anumite domenii. Ceea ce e numii atât de des „suveranitate naţională" poate fi considerat, în realitate, ca fiind compus din mai multe straturi: *suveranitatea etilica*, în carc puterea politică rezidă doar în mâinile unor cetăţeni aparţinând unui grup etnic, *suveranitatea lingvisticăf* în care puterea aparţine celor care posedă anumite priceperi lingvistice şi *suveratitatea culturală*, în care caracteristicile unui stat-naţiune sunt definite în termenii moştenirii sale culturale şi un atac asupra acesteia este considerat a fi un atac la suveranitatea statului însuşi. Acest lucru se poate vedea în cazul Franţei, în care guvernul a făcut eforturi considerabile pentru a stopa importul culturii americane.

Un alt element al suveranităţii naţionale este *suveranitatea informaţională*, în care un stat-naţiune tinde să controleze fluxul informaţional în cadrul statului şi în afara graniţelor sale. O consecinţă a revoluţiei informaţionale a constituit-o creşterea inabilităţii statului de a controla fluxul imaginilor şi ideilor, carc modelează gusturile şi valorile umane.

În ceea ce priveşte conceptul de *ciberspaţiu*, este evident că noţiunea de *frontieră* devine irelevantă din ce în ce mai mult. Cum pot statele să asigure integritatea sistemelor lor? Pot să insiste asupra standardelor minime ale comportamentului etic al cetăţenilor lor, în privinţa materialelor disponibile gratuit, sau va fi vorba de o gratuitate pentru toţi?

Globalizarea infrastructurii informaţionale repune în discuţie conceptul de stat-naţiune, în cazul în care, de exemplu, o organizaţie, care îşi desfăşoară activitatea într-o anumită ţară arc aceleaşi viziuni politice ca cele ale unei alte ţări.

London 1991.

Paul Kennedy credea că: „adevăratul motiv al existentei unei frontiere este ca nimeni să nu aibă controlul absolut, cu excepţia, poate, a managerilor corporaţiilor multinaţionale, a căror respon sabilitate este îndreptată către acţionari, care, se poate spune că au devenit noii suverani, şi investind într-o companie, dau ccle mai mari profituri”[112].

Conceptul de suveranitate se află, de aceea, sub o mare presiune şi nu mai corespunde dezvoltării globale a infrastructurilor informaţionale.

Rolul informaţiei în zilele noastre nu e foarte diferit de cel pe care-l avea în trecut. Avem nevoie de informaţie pentru a putea lua decizii, pentru a interacţiona social şi pentru a trăi. Ceea ce s-a schimbat, totuşi, este natura cantitativă a informaţiei şi, după cum remarca Stanislaw Lem, un filosof polonez, „timpul marilor politicieni a trecut pentru că fluxul informaţional face imposibil, prea complicat procesul decizional”[113].

Problema integrităţii informaţiei, când se confruntă cu un astfel de flux informaţional, devine critică şi decidenţii trebuie să ştie care informaţie e validă, care e coruptă, care e relevantă şi care ar trebui ignorată. Procesarea modernă a informaţiilor, după cum am văzut, e vulnerabilă şi informaţia poate fi coruptă, distrusă sau modificată în timpul ei.

Ritmul schimbărilor tehnologice pare să nu încetinească şi multe din problemele ridicate aici vor trebui abordate în viitorul apropiat dacă vom dezvolta calităţile necesare, modelele şi metodologiile care să fie capabile să cuantifice ameninţările la care sunt supuse sistemele.

Consecinţele ignorării acestor probleme vor fi foarte mari. Acestea trebuie să devină un subiect de reflecţie pentru întreaga societate şi nu doar a unui singur grup concentrat asupra problemelor tehnologiei informaţionale.

---

112 Paul Kennedy, Preparing for the Twenty-First Century, New York, Vintage Books, 1994.

113 Stanislaw Lem, The Times Magazine, 11.05.1996.

Spectrul cunoaşterii poate fi foarte folositor.

Ne-am concentrat atenţia în acest material asupra informaţiei, fluxului informaţional, integrităţii informaţionale şi managementului informaţional. Însă ce va trebui să facem de acum încolo este să ne aplecăm asupra procesului prin care această informaţie este utilizată de creierul uman. Este posibil să fim asistaţi în acest proces de inteligenţă artificială şi de tot ceea ce ar putea urma acesteia. Trebuie să încercam să răspundem la dificila întrebare: cum putem face să restabilim abilitatea factorilor de decizie din oricare domeniu de a lua decizii, bazându-se pe un grad de confidenţă, de integritate şi de relevanţă a informaţiei?

ANEXA 1

NETWORK CENTRIC WARFARE – Un concept controversat – Netwok Centric Warfare

NCW se fundamentează pe experienţa acelor organizaţii care s-au adaptat cu succes la presiunile exterioare intrinseci Erei Informaţionale. Studierea conceptului de Network Centric Warfare ne conduce la o concluzie majoră, şi anume aceea că adaptarea presupune schimbarea metodelor.

NCW recunoaşte importanţa informaţiei, potenţialul de putere al acesteia. Acest potenţial este rezultatul direct al relaţionărilor inter-individuale, inter-organizaţionale şi al proceselor dezvoltate de aici. Aceste noi tipuri de relaţii creează noi tipuri de comportamente şi moduri de operare.

NCW furnizează o nouă perspectivă de analiză a misiunilor militare, a operaţiilor şi a organizaţiilor, centrată pe găsirea soluţiilor inteligente prin depaşirea ideilor preconcepute.

Acest capitol începe prin a defini şi explica fundamentele conceptuale ale NCW.

Capitolul include şi o vedere generală prin prisma NCW asupra entităţilor care acţionează în câmpul de operaţii.

Definiţia NCW

Conceptul se defineşte prin referirea la oameni şi

organizaţii pornind de la necesitatea adoptării unei paradigme noi (gândirea *network centric*) şi aplicarea ei în sistemul operaţiilor militare.

NCW se centrează asupra puterii de luptă care poate fi generată prin eficientizarea legăturilor dintre diferite structuri de luptă. Principala sa caracteristică constă în abilitatea de dispersate geografică a forţelor în scopul cunoaşterii partajate a câmpului de luptă.

NCW sprijină comanda rapidă, convertirea informaţiei superioare în decizie.

NCW este transparent la misiune, mărimea forţei, şi factorii geografici. Mai mult, dispune de potenţial permiţând fuzionarea nivelelor tactic, operaţional şi strategic.

Pe scurt, NCW nu se limitează doar la aspecte tehnologice, ci la întregul spectru de probleme pe care le poate presupune războiul în Era Informaţională.

Ca întreprindere de tip NCW, armata corelează elemente de bază necesare generării puterii de luptă. Ca şi în sectorul economic totul începe de la Infrastructura Informaţională. Aceasta oferă posibilitatea cunoaşterii partajate a câmpului de luptă. Această „cunoaştere" constituie pârghia pentru sincronizarea forţelor şi pentru comanda eficientă.

Efectul îl reprezintă accelerarea ritmului operaţiilor.

Pentru definirea conceptului trebuie să lămurim câţiva termeni-cheie:

1. „Dispersarea geografică a forţelor". În trecut se limita la:

— abilitatea de a comunica;

— de mişcare;

— de protejare a forţelor şi a elementelor lor de sprijin aflate în locaţiile lor sau în imediata vecinătate a inamicului.

De aceea „dispersarea geografică a forţelor" era destul de slabă şi nu putea răspunde rapid în cazul atacurilor concentrata Tehnologiile specifice erei informaţionale fac posibilă eliberarea puterii de luptă din

locaţiile fizice ceea ce va conferi forţelor o mobilitate eficientă. Eliminarea constrângerilor geografice asociate cu lupta prezintă următoarele avantaje:

a. Permite trecerea de la abordarea bazată pe comasarca trupelor la cea bazată pe efectele de luptă.

b. Nu mai este necesară concentrarea forţelor deoarece abilitatea de comunicare a informaţiilor este extrem de rapidă şi nu mai este limitată de constrângerile geografice.

c. Permite ştergerea urmelor reducând astfel riscul de a fi descoperiţi de adversar. Conceptul de *manevră* se extinde prin reducerea nevoilor de transport a obiectelor fizice, consumatoare de bani şi de timp.

Cu NCW putem avea acclaşi lucru în mai multe locuri şi la momente diferite. Accasta pentru că un anumit senzor sc poate afla într-o poziţie care vizează mai multe ţinte fără să fie deplasat.

2. „Intelligent” Acest termen desemnează puterea dată de deţinerea informaţiei, derivată din partajarea cunoştinţelor despre câmpul de luptă şi înţelegerea intenţiilor comandanţilor, din sincronizarea proprie, din ştergerea urmelor.

O forţă inteligentă sc bazează pe informaţie oportună şi viabilă precum şi pe existenţa instrumentelor de proccsarc şi expertiză necesare.

3. „Legături eficiente” între entităţile aliate în câmpul de operaţii. Aceasta presupune:

a. Entităţile dispersate şi distribuite care pot genera sinergie b. Responsabilităţile şi munca care le poate dinamiza în scopul adaptării la situaţii. „Legăturile eficiente” necesită existenţa unei infrastructuri informaţionale robuste care să furnizeze tuturor elementelor acces la informaţie. Mecanismele şi procesele care creează aceste „legături eficiente” determină coeficientul de putere şi de multiplicare. Natura legăturilor care furnizează cea mai bună performanţă pe tot spaţiul de operaţii constituic o problemă foarte importantă. Scopul este acela de a construi o configuraţie care să asigure

eficienţa forţelor.

Aşa cum a fost definit mai sus, NCW reprezintă cel mai adecvat termen care poate descrie evoluţia cea mai probabilă a conceptului de *război* în Era Informaţională.

NCW recunoaşte natura dinamică şi complexă a războiului. NCW oferă comandanţilor o nouă abordare, mai flexibilă. Flexibilitatea operaţională va putea răspunde provocărilor Erei Informaţionale.

Conceptifl de NCW nu presupune, aşa cum cred greşit unii, numai comunicarea prin intermediul reţelelor de computere. NCW reprezintă un mijioc pentru atingerea unui scop.

El face legătura dintre diferitele state majore aflate în spaţii geografice diferite. NCW nu se concentrază pe tehnologie ci pe fluxul informaţional, pe natura entităţilor aflate în spaţiul de operaţii şi pe interacţiunea dintre ele. NCW reflectă şi încorporează caracteristicile necesare pentru eficienţă în Era Informaţională.

Puterea NCW

NCW se centrează pe avantajele oferite de partajarea informaţiilor privind câmpul de operaţii, caracteristică ce reiese din însuşi titulatura termenului. Aceasta permite obţinerea efectelor sinergice. NCW este construit în jurul conceptului de „partajare a informaţiilor", „punere în comun a informaţiilor" Doar reţeaua face posibilă o astfel de partajare (*sharing*).

O reţea constă în noduri şi legăturile dintre noduri. Nodurile constau în lucruri (decizii, acte) şi informaţii.

Legătura dintre entităţile aflate în câmpul de operaţii vor determina creşterea eficienţei operaţiilor. Experienţa dün sectorul civil ne-a arătat în ce mod materia poate fi substituită cu informaţia şi cum, fără să mişti oameni, poţi deplasa numai informaţii. Acestea duc la reducerea resurselor materiale şi de timp.

Pentru a înţelege NCW trebui să vedem în ce mod operează nodurile în legătură cu o ţintă. Pentru aceasta se execută următorii paşi:

Detectarea ţintei;

Identificarea ţintei;
Decizia de a ataca ţinta;
Transmiterea deciziei;
Lansarea armei şi deschiderea focului asupra ţintei.

Pentru acestea trebuie stabilite: timpul şi nivelul de luptă.

Timpul se stabileşte în funcţie de următorii factori:

1. gradul de mobilitate a ţintei,
2. contramăsurile adoptate de ţintă,
3. natura senzorilor şi a armamentului,
4. gradul de procesare a informaţiilor,
5. procesul decizional.

Nivelul de luptă se stabileste în funcţie de:

1. caracteristicile senzorilor şi armelor,
2. de consumul de timp pe care îl presupune.

În operaţiile de luptă performanţa capabilităţilor combinaţiei dintre senzori şi armament este în primul rând guvernată de învelişurile platformei centrice de angajare create numai atunci când platformele având la bord senzori asigură o calitate a cunoaşterii. Pentru luptători, ţinta este în cadrul învelişului de angajare maxim al armamentului.

Un înveliş efectiv de angajare este zona definită de suprapunerea parţială a calităţii cunoaşterii şi învelişul care reprezintă implicarea maximă a armamentului.

Ca urmare puterea de luptă instantanee pentru ca o platformă centrică să fie angajată este proporţională cu învelişul de angajare efectiv.

În operaţiile NCW puterea de luptă este adesea limitată de către inabilitatea platformei de a genera o cunoaştere de calitate care să fie folosită la angajarea acţiunilor într-o măsură mai mare sau egală decât maximum învelişului de angajare a armamentului.

Această situaţie apare frecvent în angajamentele platformelor NCW din luptele aeriene ca rezultat al inabilităţii unui echipaj al unei aeronave de a identifica rapid şi eficient dacă mijloacele aeriene care îl înconjoară sunt amice sau inamice şi dacă ceea ce descoperă şi

urmăreşte este ca atare detectat de senzori.

În marea majoritate a operaţiilor luptătorii, trăgătorii, sunt angajaţi în conjuncţie cu capabilităţile de comandă şi control. Situaţiile operaţionale care există atunci când o platformă centrică de tragere este legată de un nod de comandă şi control cu capabilităţi de senzori prin intermediul unor legături prin voce pot fi în practică diferite. Nodul de comandă şi control este capabil să dezvolte un nivel al cunoaşterii situaţiei limitat, bazat pe informaţiile asigurate de către senzori care pot să fie dispuşi în cadrul nodului C2, sau extern.

În cele mai multe situaţii nivelul de cunoaştere disponibil al nodului C2 este calitativ suficient pentru a conduce un trăgător într-o zonă de angajare, dar insuficient pentru a-i permite trăgătorului să fie dirijat direct.

Mai departe, câtă vreme legătura dintre platformele C2 şi platforma centrică de tragere este o legătură prin voce, tot schimbul de informaţii dintre acestea trebuie să aibă loc tot prin voce.

Pentru exemplu, în lupta de combatere a operaţiilor aeriene, ofiţerul cu armamentul aflat la bordul unei aeronave E – 2 Hawkeye sau al unui E – 3 AWACS, nu trebuie să aibă în mod necesar o calitate anume a cunoaşterii pentru a angaja acţiunile contra tuturor obiectelor care sunt urmărite.

În mod tipic, fiecare incertitudine asociată poziţiei unei ţinte potenţiale este mare, sau informaţia disponibilă este insuficientă pentru a identifica în mod cores-punzător o ţintă.

În consecinţă echipajul unui avion de vânătoare trebuie să aibă senzori la bord care să asigure o cunoaştere a situaţiei de calitate şi care să permită şi acţiunea, respectiv executarea atacului cu armamentul din dotare.

Mai mult, câtă vreme toate informaţiile schimbate au loc prin voce, poate fi extrem de dificil pentru echipele din nodul C2 şi platformele de tragere să dezvolte şi să

menţină o cunoaştere a situaţiei atunci când există un număr mare de mijloace ale forţelor albastre sau roşii care operează într-o zonă apropiată.

Prin comparaţie operaţiile de reţea centrică din NCW, capabilităţile de sesizare, de comandă, de control sau de angajare sunt strâns legate şi lucrează în reţea prin intermediul datelor digitale. Sursa acestei puteri sporite în operaţiile de reţea centrică derivă în parte din conţinutul sporit, calitatea şi oportunitatea fluxurilor de informaţii dintre noduri în cadrul reţelei.

Această sporire a fluxului de informaţii este esenţială pentru a permite partajarea cunoaşterii situaţiei din câmpul de luptă şi pentru sporirea acurateţei informaţiilor.

Experienţa operaţională cu date, cu legături digitale, de nivel tactic, dovedeşte puterea operaţiilor în reţeaua centrică.

Într-un experiment care a comparat performanţa operaţionala a lui F15 îndeplinind o operaţie de luptă aeriană cu şi fără legături de date, forţa aeriană a descoperit cum prin întrebuinţarea reţelelor NCW coeficientul de letalitate sporeşte ajungând până la 100%.

Această putere de luptă sporită a rezultat din semnificativa sporire a cunoaşterii situaţiei din spaţiul de luptă care a fost asigurată piloţilor care au operat cu date de legătură tactice.

Componentele cunoaşterii situaţiei din câmpul de lupta includeau performanţa armamentului forţei albastre (un exemplu), poziţionarea în timp real a albaştrilor şi forţelor roşii, starea, situaţia, acţiunilor, în desfăşurare a albaştrilor.

Rezultatul evident a lost o îmbunătăţire semniJ'icativă a capabilităţilor de a observa, orienta, decide şi acţiona. Constatările recente ale echipei de evaluare şi identificare a serviciului de luptă au confirmat toate acestca.

De exemplu o situaţie „A" care prezintă două platforme centrice de tragere ce operează în proximitate susţinute de senzori externi care pot să asigure informaţii

specifice.

Într-o astfel de situaţie informaţia despre acţiunile desfăşurate în timp real nu poate fi partajată efectiv iar puterea de luptă nu este maximizată.

Prin contrast în situaţia „B" valoarea adăugată a puterii de luptă asociată cu o operaţie NCW în acest mod de operare o partajare a informaţiei aproape în timp real între noduri, dezvoltă mult puterea de luptă.

Lucrul fiabil în reţea, al senzorilor asigură forţei capabilitatea de a genera o cunoaştere partajată mărind în acelaşi timp şi calitatea. Această cunoaştere sporită este proporţională cu întreaga zonă acoperită de către senzorii zonali, putând fi exploatată de către un fiabil lucru în reţea al C2 şi de către entităţile, actorii din zonă, care pot astfel să coopercze, şi să-şi autosincronizcze forţele.

Potenţiala sporire a puterii de luptă în ansamblu, asociată cu operaţiile NCW este dată de mărirea suprafeţei învelişului de acţiune efectivă.

Nu putem păstra forma simplă a lucrurilor din întregul spaţiu de luptă fără o organizare corespunzătoare şi fără schimbări doctrinare care să mărească eficienţa în desfăşurare a acţiunilor de luptă.

Practic, există consecinţe neintenţionate ale conectării spaţiului de luptă şi în speranţa de mai bine, de fapt putem degrada performanţa în mod particular dacă schimbăm neadecvat doctrina, organizarea, instruirea şi alte elemente cheie ale procesului.

De aceea drumul către un război bazat pe NCW are nevoie să fie îmbogăţit cu analize şi experimente în scopul de a înţelege cum putem beneficia cât mai mult de pe urma potenţialului imens al NCW în timp ce evităm consecinţele neintenţionate.

Măsura în care productivitatea lucrului în reţea depăşeşte suma productivităţii părţilor sale depinde de două lucruri.

Primul este câştigul şi poate fi obţinut prin simplă partajare a resurselor (informaţiei) din cadrul nodurilor.

În mod evident nu toate organizaţiile au probabilitate

egală de a avea informaţiile de care au nevoie.

Aceasta la momentul de faţă lucrează în favoarea noastră, pentru că noi folosim cunoştinţele despre organizaţiile şi indivizii care sunt cel mai probabil în măsură să-şi obţină informaţiile care le trebuie.

Având dezvoltate aceste capabilităţi, puncte de comandă şi informaţii inteligente pentru planuri, putem, folosind puterea lucrului în reţea să transformăm o probabilitate foarte scăzută de a avea o infor-maţie într-una foarte mare.

Acesta este practic aspectul la care se gândesc cei mai mulţi oameni atunci când se referă la puterea lucrului în reţea, dar este totodată vorba şi de o nouă ipoteză fundamentală care sugerează că deblocarea întregii puteri a lucrului în reţea implică afectarea naturii deciziilor care sunt în mod inerent făcute prin intermediul reţelelor.

Aceasta poate să nu fie imediat distinctă câtă vreme acestc decizii colective sunt adesea implicite şi de aceea nu tocmai vizibile.

Este necesar să acordăm mai multă atenţie comportamentului entităţilor care lucrează în reţea, mai curând decât să studiem şi să considerăm comportamentul entităţilor individuale. Rezultatele Flotilei Delta de Luptă Experimentală, oferă suport pentru acestc ipoteze.

Este axiomatic aproape pentru orice situaţie că putem de fiecare dată să facem în aşa fel încât, măcar până la limita constrângerilor să fie bine, să ne îmdreptăm spre succes.

Cu toate acestea, nu de puţine ori constrângerile sunt folosite ca mijioace de a obţine rezultate care adesea sunt importante obiective ale sarcinilor primite.

De exemplu, ne referim la nişte actori însărcinaţi să atace un număr de ţinte.

Costrângerile asupra opţiunilor sunt adesea folosite ca mijioace de a reduce fratricidul chiar dacă vor reduce probabil şi numărul de ţinte doborâte şi vor mări riscul ce l-ar presupune pierderea secretului acţiunilor.

Scopul NCW în această situaţie este de a obţine o

reducere a probabilităţii de fratricid, concomitent cu minimizarea constrângerilor cu privire la folosirea armamentului.

O modalitate de a reuşi acest lucru este de a face actorii să fie mult mai înştiinţaţi, informaţi, iar armamentul acestora tot mai inteligent.

În operaţiile de luptă capacităţile performante ale armelor cu senzori sunt guvernate de teren, de „argumente geometrice” (Platform-Centric Engagement Envelope

Astfel:

1. un factor de decizic fără constrângeri (limitări) informaţionale.

2. câţiva factori de decizie, fiecare cu viziuni limitate şi cu informaţii procesate limitate.

Hai să luăm în considerare cazul când un singur decident poate cunoaşte informaţiile comune despre ţintă, în sensul că deţine tabloul complet al câmpului de operaţii şi timpul necesar procesării şi transmiterii ordinelor fiecărui actor implicat.

În aceste condiţii decizia optimă poate fi influenţată. În astfel de cazuri funcţia reţelei este aceea de a contribui la creearea unui tablou complet prin asamblarea descrierilor parţiale şi de a transmite aceste informaţii (cunoştinţe) de la factorii de decizie către fiecare actor implicat.

Cu alte cuvinte nodurile senzori, partajează fiecare informaţiile lor cu nodul decizional, care la rândul lui partajează decizia cu actorii implicaţi în fiecare nod. Totuşi în viaţa reală acest lucru este puţin probabil să se producă aşa de eficient.

Rareori se pot lua decizii optime. Pentru oricine decizia optimă centralizată reprezintă un obiectiv foarte greu de atins.

Pentru NCW lucrurile nu stau deloc aşa.

Observăm că puterea NCW derivă din împuternicirea tuturor factorilor de decizie nu doar a câtorva. Dimensiunile complexe şi ritmul operaţiilor trebuie să ne

conducă în cele din urmă la utilizarea reţelelor.

Obiectivul este acela de a implica toţi actorii în acelaşi tip de joc şi la timpul oportun. În ceea ce priveşte controlul, NCW nu conduce automat la controlul centralizat.

Pe de o parte NCW amplifică cunoaşterea pentru toate entităţile implicate, pe de altă parte duce la descentralizarea deciziei şi a controlului. După cum se aplică NCW în managementul informaţional al câmpului de operaţii ne putem aştepta, în termeni absoluţi, că fiecare entitate va deţine mai multe informaţii despre acesta.

În viitor ne putem aştepta ca la nivel tactic comandanţii vor avea o mai bună înţelegere asupra caracteristicilor câmpului de operaţii şi a necesităţilor de instruire.

Colaborarea virtuală în acest capitol vom examina natura beneficiilor ce pot li obţinute prin partajarea informaţiilor şi bunurilor. Mai devreme ideea a fost aceea că un lucru robust în reţea al ecosistemului de ducere a acţiunilor de luptă permite unor lucruri şi sisteme de relaţii noi să se dezvolte.

Un astfel de produs, dintre cele mai puternice, care rezulta într-un asemenea câmp de luptă este colaborarea virtuală.

Colaborarea virtuală este mai mult decât simpla partajare a informaţiilor; ea permite elementelor unui ecosistem de ducere a acţiunilor de luptă să interacţioneze şi să colaboreze în domenii virtuale, să „mişte” informaţia în loc de a „mişca” oamenii şi sa obţină un nivel de cunoaştere critic în rândul maselor.

Compo-nentele tehnologice cheie cum ar fi videoteleconferinţa şi aplicaţiile de planificare colaboraţive permit o colaborare virtuală. Colaborarea virtuală în domeniul informaţional are numeroase beneficii operaţionale.

De exemplu, o colaborare virtuală permite timpului asocial procesului de planificare şi executare existent să fie mult mai redus Aceste economii, ulterior, înseamnă

timp suplimentar pentru executarea unor antrenamente, deplasări la contact sau odihna trupelor. Rezultatul final se regăseşte în sporirea eficienţei.

În operaţiile expediţionare aerospaţiale „mişcarea” informaţiei în locul oamenilor schimbă mult dinamica forţei şi proceselor desfăşurate permiţând derularea unor operaţii independente. Conceptul s-a dovedit promiţător de exemplu în timpul Forţei Expediţionarc Experiment '98.

Operaţiile independente pot reduce atât timpul necesar pentru a iniţia operaţia aeriană, cât şi pentru a rentabiliza transportul aerian pentru a deplasa capabilităţi de luptă în teatru.

Abilitatea de a „mişca” informaţia în locul luptătorilor are totodată beneficii semnificative şi în alte domenii.

Cunoaşterea Câmpului de Operaţii

NCW dezvoltă şi menţine capacităţile de cunoaştere a caracteristicilor câmpului de operaţii prin colectarea, procesarea şi diseminarea informaţiilor.

Aceasta presupune partajarea şi fuzionarea informaţiilor întrun aşa numit COP sau altfel spus (*Common Operaţional Pictore*)

Furnizarea către trupele întrunite a cunoştinţelor oportune şi viabile despre spaţiul de luptă presupune colectarea datelor şi informaţiilor din surse multiple, procesarea în care este inclusă şi analiza, transportarea, fuzionarea, plasarea în context şi prezentarea în modul cel mai adecvat.

De asemenea, este necesară instruirea în acest sens a entităţilor şi actorilor implicaţi în procesul decizional.

În concluzie, putem observa că NCW preupune atât cunoaşterea spaţiului de operaţii cât şi a modelelor cognitive care permit această cunoaştere.

Informaţii incluse într-un astfel de tablou reprezentativ al câmpului de operaţii pot fi următoarele:

Locaţia (poziţiile curente, gradul de mobilitate, predicţii legate de poziţiile viitoare);

Statutul (gradul de operabilitate, capacităţile de

luptă, susţinerea logistică, etc.);

Cursul acţiunii actuale şi predicţia celei viitoare a inamicului(capacităţile ofensive şi defensive ale adeversarului, evaluarea pagubelor, etc.);

Mediul (condiţiile atmosferice actuale şi viitoare, efectul vremii asupra operaţiilor, caracteristicile terenului cum ar fi gradul de circulare, liniile de vizibilitate, etc.)

Partajarea acestor informaţii presupune accesul tuturor forţelor la Tabloul Operaţional Comun. Informaţiile despre spaţiul de operaţii trebuie considerate ca o proprietate comună (un fel de conştiinţă colectivă). Ea trebuie să funcţioneze nu doar în cadrul unui nod, ci în toate nodurile relevante din toate eşaloanele şi componentele funcţionale.

Conţinutul informaţiilor din tabloul operaţional necesare factorilor de decizie poate varia în funcţie de eşaloane..

Partajarea cunoaşterii situaţiei din câmpul de luptă apare atunci când elemente relevante ale ecosistemului de ducere a războiului sunt asigurate cu acces la COP (imaginea comună operaţională).

Practic, cunoaşterea situaţiei din spaţiul de luptă trebuie să fie văzută ca pe o proprietate colectivă. Nu există numai un singur loc (nod) în spaţiul de luptă, şi mai mult, toate nodurile din spaţiul de luptă din cadrul eşaloanelor sau din cadrul componentelor funcţionale pot fi relevante. Gradul de detaliere care este ilustrat în imaginea operaţională comună poate să fie însă diferit de la eşalon la eşalon.

Gradul în care conţinutul informaţiei dintr-un cadru operaţional poate să varieze în funcţie de eşalon. Informaţia pentru a genera cunoaşterea situaţiei din spaţiul de luptă va fi asigurată din numeroase surse.

De exemplu, informaţia din cadrul forţelor roşii poate să fie culeasă prin intelligence, supraveghere şi platforme de recunoaştere care operează ca parte a senzorilor de reţea, senzori angajaţi în platforme de armament, sau oamenii, agenţii din teren (trupele de cercetare).

O partajare a cunoaşterii poziţiilor albaştrilor în cadrul spaţiului de luptă poate să fie generală prin permiterea tuturor elementelor forţelor albastre de a transmite informaţii despre poziţii actuale şi de a recepţiona informaţii despre poziţii relevante cu privire la alte entităţi.

Fiecare element al forţelor albastre poate să stabilească poziţia sa în spaţiul de luptă cu un mare grad de precizie prin folosirea sistemelor de navigaţie specifice cum ar fi sistemul de poziţionare global (GPS).

Despre situaţia forţelor albastre, cum ar fi situaţia carburanţilor sau performanţa armamentului, aceasta poate să fie generată prin folosirea unor senzori încastraţi, sau de teren, care să urmărească de pildă consumul de carburanţi sau efectele artileriei.

Operarea cu date în timp aproape real poate fi de asemenea luată în calcul, contribuind la menţinerea dinamicităţii sau a gradului de operativitate la nivel operaţional prin stabilirea cu anticipaţie şi precizie a unor nevoi de întreţinere.

Mediul informaţional poate fi conectat prin diferite tipuri de senzori tradiţionali cărora să le fie sporit potenţialul prin informaţiile primite de la senzorii de pe platformele de armament.

Generarea de cunoaştere a situaţiei partajată a albaştrilor necesită un mecanism în locul „capturilor” de dinamicitate, poziţie, situaţie sau informaţii, despre intenţia sa de la toate elementele forţelor albastre şi să avem capabilitatea de a asigura informaţii relevante doar pentru albaştrii care au într-adevăr nevoie de ele.

Pentru ca aceasta să se întâmple, toate elementele relevante ale forţelor albastre au nevoie să fie participante la proces.

Ele au nevoie să fie conectate în reţea.

În scopul de a obţine o cunoaştere a situaţiei din spaţiul de luptă şi apoi de a obţine o avertizare asupra acestuia avem nevoie Isă trecem dincolo de informaţiile care ne spun de locul lucrurilor jşi să ajungem la acele

informaţii care ne dezvăluie şi identitatea lor.

^ Este de asemenea necesar să cunoaştem câte ceva despre tftuaţia operaţiilor în desfăşurare, cum la fel de important este să Mm despre doctrină şi intenţii.

În mod similar dacă informaţiile despre forţele roşii, sau Aspectele ce ţin de situaţia acesteia, sunt obţinute de o componentă i1 forţei, pentru a genera o cunoaştere a situaţiei din spaţiul de lâptă este necesară distribuirea lor, tuturor elementelor relevante Je forţei.

Abilitatea de a dezvolta surse de informaţii precise şi oportune pentru cunoaşterea situaţiei din spaţiul de luptă depinde de caracteristicile proceselor informaţionale disponibile şi de performanţa reţelelor.

De exemplu precizia unei informaţii de poziţie distribuită cu privire la nişte ţinte mişcătoare (amice, neutre sau roşii) este în funcţie nu doar de procesele de colectare şi analiză ci de asemenea şi în funcţie de viteza de deplasare a obiectivelor sau de viteza informaţiilor din cadrul reţelelor albaştrilor.

De exemplu o platformă de armament a albaştrilor cum ar l i un AH 64 D Apache detectează o coloană de tancuri.

Senzorul aflat la bord este capabil să genereze o informaţie de calitate cu privire la acţiunea în sine şi nu neapărat de o detaliere care să indice şi numărul de tancuri inamice din respectiva coloană.

Această informaţie are o valoare potenţial semnificativă pentru forţa care luptă.

Valoarea acestei informaţii este în funcţie de posibilitatea de a o partaja şi cât de oportun se face partajarea.

De exemplu dacă Apache-ul poate să ofere o cunoaştere de calitate a acţiunii în care sunt antrenaţi militarii unei baterii de artilerie într-un timp real atunci există posibilitatea pentru forţele albastre de a comasa efectele focului direct cu cele ale focului indirect.

Dacă informaţia nu poate fi transmisă în timp real atunci oportunitatea de a comasa efectele este pierdută.

Cu toate acestca dacă informaţia despre o poziţie a unei ţinte colectată de către un Apache poate fi transmisă, dar nu în timp real, informaţia trebuie să fie suficient de precisă pentru a permite un sprijin aerian apropiat, respectiv atacarea acelei coloane de tancuri.

În mod similar dacă un comandant doreşte să sporească viteza manevrei forţelor sale, menţinând în mod simultan cunoaştere; situaţiei din spaţiul de luptă atunci viteza informaţiei trebuie sa crească odată cu viteza manevrei.

De exemplu putem observa că după cum viteza medie a forţelor albastre creşte, precizia informaţiilor de poziţie partajauva descreşte dacă viteza medie a informaţiei nu sporeşte în mod corespunzător.

Aceasta apare din cauza preciziei instantanee care este o funcţie a latenţei informaţiei. În mod simplificat folosind o rată constantă de actualizare a poziţiei, eroarea instantanee de poziţie a unei platforme de armament care se deplasează cu 500 de mile/ oră, cum ar fi viteza unui avion, este potenţial de 10 ori mai mare cum ar fi cea a unei platforme care se deplasează cu 50 de mile/ oră, cum ar fi viteza unui tanc.

În rezumat, precizia, acurateţea, unei informaţii într-o imagine operaţională comună este în funcţie de:

— exactitatea sursei de informaţii,

— viteza informaţiilor dintre nodurile din reţea

— viteza ţintelor în cadrul operaţional comun.

Abilitatea noastră de a asigura entităţilor din spaţiul de luptă accesul la informaţie poate să fie exploatată pentru a spori acurateţea sau precizia informaţiilor noastre despre bunurile inamicului.

Particularităţile despre cum o creştere a vitezei informaţiilor poate fi folosită pentru a spori cunoaşterea situaţiei din spaţiul de luptă este tratată mai jos.

Network Centric Warfare şi Funcţiile de Comandă-Control şi execuţie

Am văzut în capitolele anterioare că adoptarea şi implementarea conceptului de NCW determină o creştere

semnificativă a abilităţii de cunoaştere partajată a câmpului de operaţii.

În următorul capitol se pune accentul pe implicaţiile NCW asupra funcţiilor de execuţie şi comandă-control.

Natura funcţiei C2 constă în capacitatea comandantului de a înţelege şi controla orice situaţie. În acest scop comandanţii sunt instruiţi cu acele cunoştinţe necesare exercitării funcţiei de C2.

Out-put-urile funcţiei de comandă-control constau în:

1. decizii adoptate în funcţie de percepţia comandanţilor asupra situaţiei şi de intenţiile lor;

2. executarea deciziilor.

Acest capitol se centrează pe relaţia dintre partajarea informaţiilor prin intermediul NCW, eficienţa deciziilor şi a implementării lor. Folosind conceptele tipice NCW se poate obţine un grad foarte înalt de cuplare între C2 şi controlul focului.

Această cuplare strânsă care permite translatarea până la cele mai înalte nivele a informaţiilor partajate despre câmpul de operaţii generează creşterea puterii de luptă. Aceasta poate fi obţinută prin multe modalităţi: planificarea şi execuţia, operaţiile de distrugere, sincronizarea operaţiilor. Astfel de exemple vor fi prezentate pe parcursul acestui capitol.

NCW furnizează oportunităţi de îmbunătăţire a funcţiilor C2 şi de execuţie la nivelul fiecărui eşalon în contextul misiunilor specifice deoarece:

Entităţile decizionale sau elementelor specifice C2 vor deţine mai multe cunoştinţe;

Actorii implicaţi vor deţine mai multe cunoştinţe;

Actorii şi entităţile decizionale vor fi mult mai bine conectate;

Elementele de avertizare vor fi mult mai responsabile;

Urmele lăsate vor deveni din ce în ce mai mici.

Fiecare din aceste îmbunătăţiri vor face posibilă înţelegerea diferenţiată a lucrurilor. Trebuie să conştientizăm că proprietăţile NCW oferă oportunitatea

armonizării eficiente între abordarea asupra caracteristicilor câmpului de operaţii şi a condiţiilor de obţinere a eficienţei la cele mai înalte nivele.

Entităţile decizionale „intelligente” vor fi capabile să abordeze problemele într-un mod diferit faţă de acele entităţi mai puţin „intelligente” Procesul decizional nu se va mai concentra pe abordarea defensivă care presupunea adoptarea măsurilor de securitate împotriva incertitudinilor ci pe dimensiunea proactivă.

Partajarea cunoştinţelor va determina delimitarea distinctă a capacităţilor adversarului. Aceasta presupune să acordăm mai multă atenţie modelării câmpului de operaţii şi mai puţină atenţie la reacţia şi la schimbările bruşte sau neaşteptate.

Astfel planificarea va presupune mai multă economie de energie şi resurse. C2 şi execuţia vor deveni un proces integrat în care eforturile vor fi canalizate pe monitorizarea implementăm deciziilor şi modificărilor în timp real.

Entităţile inteligente vor transforma abordarea privind funcţia de comandă-control de la un proces rigid de planificare şi decizie la un proces de transmitere a scopurilor şi intenţiilor şi de orchestrare a sprijinului necesar executării deciziilor. Pe măsură ce se renunţă la detalii viteza de comandă va creşte. Mecanismul C2 va fi redus la nevoia de informaţie ceea ce va contribui la creşterea mobilităţii.

O mai bună conectivitate între actori şi entităţile decizionale va genera creşterea capacităţii de reacţie la modificările de situaţie. Mobilitatea se va extinde în condiţiile în care entităţile responsabile cu procesul de avertizare vor avea mai multă putere de decizie.

Capacitatea de reacţie la modificările de situaţie va avea implicaţii profunde pentru C2 şi pentru activitatea de planificare. Planificarea va deveni un proces mult mai uşor cu cât mai mulţi factori vor fi responsabili de acest lucru.

Capacitatea de optimizare a operaţiilor va tinde să facă din planificare un proces continuu care se va îmbina,

în anumite circumstanţe, cu procesul de executare.

La orice nivel dat, aceste schimbări vor modifica radical natura proceselor de comandă-control prin acordarea de responsabilităţi eşaloanelor inferioare. În ciuda creşterii ritmului de executare a operaţiilor, entităţile decizionale de la cele mai înalte nivele vor beneficia de mai mult timp şi resurse necesare monitorizării situaţiei, identificării problemelor care apar şi rezolvării cât mai rapide a acestora.

NCW oferă nu numai oportunitatea de rezolvare sincronizată a operaţiilor ci şi de examinare a proceselor de C2 fondate pe coordonarea orizontală, de sincronizare proprie a entităţilor implicate.

Aceasta adaugă o nouă dimensiune proceselor de comandăcontrol. Este recunoscut faptul că un anumit tip de comportament organizaţional poate fi influenţat sau chiar controlat fără probleme de sus în jos. NCW oferă alternativa obţinerii rezultatelor dorite prin altă metodă. Comportamentul organizaţional reprezintă o proprietate emergentă care derivă din:

intenţiile comandantului (interiorizate de actorii implicaţi);

din gradul de cunoaştere a câmpului de operaţii;

capacitatea entităţilor decizionale de a gestiona şi diminua constrângerile determinate de alocarea limitată a resurselor. Este dificil de supraestimat impactul pe care această nouă dimensiune a C2 îl va avea asupra viitorului mod de desfăşurare a operaţiilor.

Câmpul de operaţii al viitorului, din punctul de vedere al dimensiunii şi naturii, va fi mult mai complex. Procesul de comandă-control se va confrunta cu această nouă dimensiune complexă.

Până nu demult se considera că, dacă dispunem de tehnologic avansată şi de mecanisme organizaţionale sofisticate, putem deveni stăpâni pe situaţie.

Se consideră că, dacă putem înţelege procesele de la bază putem manevra cu uşurinţă orice situaţie la orice nivel printr-o eforturi şi analiză riguroasă. Iar dacă avem

destul timp şi energic intelectuală putem dezvolta un anumit nivel de înţelegere necesară operaţiilor eficiente.

Azi mulţi specialişti au ajuns să pună sub semnul întrebării această viziune tradiţională a problemelor complexe. Ei au semnalat că multe din procesele simple nu pot fi modelate adecvai cu toată tehnologia modernă şi sofisticată de care se beneficiază.

Gestionarea sistemelor şi situaţiilor complexe este corelată inerent cu procesele de comandă-control. NCW oferă posibilitatea de a deveni stăpâni pe situaţie şi de a depăşi comportamentele aberante ale sistemului.

NCW oferă, de asemenea, posibilitatea de a compara şi îmbina procesele decizionale ierarhice, caracteristice perioadei industriale, cu modelele descentralizate care acordă putere de decizie unităţilor mici.

Noua viziune asupra procesului C2 se bazează pe coroborarea acestor două tipuri de modele decizionale, utilizate fie separai, fie simultan, în funcţie de tipul de misiune. Viitoarea arhitectură a procesului de comandă-control, modalitatea de îndeplinire a fiecărei misiuni, funcţia şi misiunea vor fi gestionate astfel încal să fie acoperit tot spectrul de probleme şi comportamente.

Cu alte cuvinte, scopul procesului de comandă-control – acela de realizare a eficienţei forţelor – va fi atins luând în calcul riscurile care trebuie aduse la nivelul de acceptabilitate, de la toate nivelele de comandă.

Există mai multe modalităţi de a lua în considerare riscurile. Astăzi se înregistrează amplificarea riscurilor neliniare care determină creşterea complexităţii câmpului de operaţii. Efectele ameninţărilor neliniare se manifestă disproporţionat în funcţie de modificarea diferitelor variabile.

Dacă într-o organizaţie (sistem) predomină comportamentul liniar-determinist, o modificare minoră în cadrul structurii (input) va determina efecte minore (output). Într-un sistem neliniar în care predomină discontinuitatea, o modificare mică poate avea efecte majore (output) asupra structurii sistemului care se poate

transforma ireversibil.

Putem translata această teorie asupra câmpului de operaţii care se va confrunta în viitor cu presiuni diferite de cele de până acum. Procesul tradiţional de comandă-control urmărea să desfăşoare lupta cu număr redus de victime umane. Abordarea actuală asupra C2 urmăreşte să diminueze erorile şi să reducă gradul de vulnerabilitate la riscuri.

Dar, pentru era informaţională nici această abordare nu mai este valabilă deoarece se bazează pe un număr redus de informaţii şi pe importanţa forţelor.

La momente diferite au fost adoptate abordări diferite care răspundeau cel mai bine condiţiilor momentului istoric respectiv.

Astăzi, în condiţiile creşterii galopante a ritmului schimbării, se urmăreşte reducerea riscurilor asociate ameninţărilor neliniare precum şi transformarea acestora în oportunităţi de exploatat în favoarea forţelor proprii, în vedere eficientizării operaţiilor.

Viteza de comandă în abordarea noastră asupra procesului de comandă-control (organizaţie, sistem) o măsură de bază constă în viteza de comandă, sau timpul necesar recunoaşterii şi înţelegerii situaţiei, identificării sau evaluării alternativelor, selectării opţiunii celei mai optime şi implementării prin ordin (comandă).

Dacă alternativa este corectă, planificarea va fi eficientă. Replanificarea este un proces consumator de timp şi de resurse ceea ce reduce eficienţa operaţiilor. Un prim pas în tot acest proces îl reprezintă înţelegerea corectă a problemei.

În operaţiile tradiţionale, cunoştinţele sunt temporare deoarece totul se schimbă în ritm foarte rapid. Un motiv pentru care planificarea iniţială nu are efectul scontat constă tocmai în această lipsă de informaţii cu valoare adăugată. Mai ales la nivelul eşaloanelor inferioare necunoaşterea situaţiei duce la eşuarea planificării iniţiale şi la întârzierea procesului decizional.

NCW duce în schimb la creşterea vitezei de decizie şi

comandă. Aceasta a fost ilustrată în timpul crizei din Taiwan, în 1995, când China a încercat să influenţeze alegerile prin manifestări şi ameninţări zgomotoase.

Aceasta până în momentul intervenţei americane cu două grupuri de armate. Pentru demonstraţia noastră ceea ce este interesant este tocmai această modalitate diferită de exercitare a funcţiei de comandă-control.

Natura structurii comenzii la nivelul amiralităţii s-a modificat în momentul în care vice-amiralul Clemins, comandantul Flotei a 7-a a decis să reducă timpul destinat planificării de la zile la ore. S-au utilizat e-mailul şi tele-conferinţa pentru a crea şi menţine la un înalt nivel gradul de cunoaştere comună a situaţiei.

S-a pus foarte mare accent pe partajarea informaţiilor în scopul eficientizării colaborării. Aceasta a accelerat procesul de sincronizare a operaţiilor desfăşurate de c4e două grupuri militare americane din Taiwan.

La nivel tactic seria de experimente desfăşurate de flota americană a demonstrat că puterea de luptă poate fi amplificată prin sincronizarea operaţiilor, prin punerea în comun a informaţiilor depre tabloul descriptiv al câmpului de operaţii.

La nivel operaţional, Doctrina întrunită pune accent pe dezvoltarea gradului de mobilitate a forţelor, menţinerea şi accelerarea ritmului operaţiilor şi angajarea prin surprindere a forţelor adversare în locurile şi momentele oportune forţelor proprii.

S-a estimat şi realizat calculul gradului de şoc, de impact asupra forţelor adversare şi de producere a confuziei în scopul dezintegrării şi anihilării adversarului.

TABLOUL OPERAŢIONAL COMUN

— cunoştinţe partajate – Un concept asociat îl reprezintă cel de *Blocare strategică*.

Reprezintă activitatea de blocare a adversarului de a-şi atinge obiectivele strategice. Chiar dacă ipoteza rămâne încă nedemonstrată, firul logicii ne conduce la ideea că blocarea strategică poate juca un rol-cheie acordând

posibilitatea de încheiere rapidă a ostilităţilor.

Repetiţia

O bună repetiţie (simulare) poate avea efecte semnificative în ceea ce priveşte creşterea gradului de combativitate. Prin exploatarea infrastructurii informaţionale tipică operaţiilor de tip NCW actorii implicaţi au acces la informaţiile comune, la instrumentele de planificare şi simulare.

Acestea oferă posibilitatea executării repetate a operaţiilor de simulare ceea ce duce la îmbunătăţirea planurilor iniţiale, la extinderea cunoaşterii şi, evident, la creşterea posibilităţii de obţinere a succesului.

Extinderea cunoaşterii

Actualele aplicaţii software (AFMSS, PowerScene, TopScene) permit actorilor din teatrul de operaţii să îşi dezvolte cunoaşterea caracteristicilor câmpului.

De exemplu, un pilot poate simula misiunea de câteva ori pentru o mai bună cunoaştere a zonei de decolare, a rutei de intrare, a rutei de ieşire, a zonei de angajare.

Ameninţările, cum ar fi staţiile de tip radar sau complexele cu rachete sol – aer (SAM) poate fi reprezentată tridimensional, permiţând pilotului să planifice şi să repete misiune pentru a diminua posibilitatea de a fi detectat de sistemele inamicului.

Aceasta conduce la creşterea posibilităţii de supravieţuire prin faptul că pilotul poate să îşi selecteze ruta de zbor astfel încât să nu fie descoperit de radare. Mai mult, simularea misiunii va permite pilotului să crească posibilitatea de identificare şi atingere a ţintei. Sau la descoperirea erorilor de planificare sau de stabilire incorectă a coordonatelor ţintei.

Fiecare din aceste exemple a fost testat în Operaţia din Bosnia (august-septembrie 1995) când au fost debarcate echipajele aeriene NATO.

Informaţiile partajate asupra câmpului de operaţii au dus la creşterea preciziei şi gradului de letalitate, la reducerea pagubelor colaterale şi la pierderi minime.

Au fost atacate cu succes 97% din ţintele vizate şi distruse 80%. Ţintele care constau în 338 de puncte vizate de lovire şi destinate atacului din interiorul a 48 de locaţii au fost studiate şi calculate pentru a se elimina pe cât posibil victimele din rândul populaţiei civile. Pe parcursul întregii operaţii a fost doborât doar un singur avion,

Mirage 2000 al cărui echipaj a supravieţuit fiind repatriat. Totul a fost posibil datorită informaţiilor oportune şi corecte privind forţele adversare şi dispunerea lor precum şi despre mediul înconjurător.

Executarea comenzii

Am văzut că prin utilizarea noului concept NCW ni se oferă posibilitatea amplificării cunoaşterii câmpului de operaţii, dezvoltării de noi abordări asupra procesului de comandă-control, de planificare şi simulare eficientă.

În finalul acestei analize trebuie să vedem în ce mod toate acestea pot fi implemetate (executate). Entităţile implicate vor avea acces la informaţie şi expertiză aşa cum am explicat în paginile anterioare. NCW le permite să comunice cu celelalte entităţi aflate în câmpul de operaţii. Dacă transmiterea mesajelor se face corect, atunci gradul de cunoaştere se va extinde, oferind oportunitatea de a fi exploatată la maximum de eficienţă.

Să presupunem că, pentru viitorul imediat, capacităţile fizice (sistemele de armament) rămân esenţiale. Această presupunere nu poate fi rezonabilă deoarece dezvoltarea sistemelor de armament necesită timp pentru transport şi desfăşurare. Această presupunere ne determină să minimizăm adevărata valoare a conceptului de NCW

Dacă el nu va fi implementat cât mai curând, se comite o eroare de proporţii. Cu alte cuvinte necesitatea este să vedem cum putem utiliza cel mai bine sistemele de armament folosind conceptele specifice NCW

Eficienţa desfăşurării actorilor în câmpul de operaţii depinde de câteva caracteristici-cheie ale acestora:

ţintele pe care le pot ataca;

expunerea la atacul adversarului (gradul de expunere

la risc);

viteza de comandă şi rata atacului pe care îl pot susţine;

responsabilitatea unităţilor de sprijin;

mobilitatea forţelor;

letalitatea forţelor;

extinderea gradului de sincronizare.

Adoptarea conceptului NCW ne oferă capacitatea de lărgire a atacului, de reducere a profilului riscului, de creştere a ritmului operaţiilor şi responsabilităţilor, de îmbunatatire a mobilităţii forţelor, de obţinere a unui grad cât mai mare de letalitate.

Superioritatea Informaţională, NCW şi avantajul cunoştinţelor (informaţiile cu valoare adăugată)

Acest raport tratează un fenomen socio-cultural care a apărut în domeniul Apărării care a devenit o problemă comună, aceea că succesul unui război modem se realizează numai dacă este obţinută Superioritatea Informaţională. În rândurile care urmează se urmăreşte demontarea acestei afirmaţii. Argumentele pornesc de la lucrări de referinţă aparţinând domeniului military cum sunt:

Începe cu o scurtă descriere a contextului socio-cultural în care a apărut acest fenomen. Descrirea se face folosind conceptecheie din lucrarea *Joint Vision 2010* şi *Strategia Politică Australiană*.

Urmează apoi o secţiune dedicată Superiorităţii Informaţionale şi Superiorităţii Cunoaştinţelor.

Succesul NCW presupune Superioritatea Cunoştinţelor utilizând Superioritatea Informaţională.

Se continuă apoi cu relaţia deosebită dintre superioritatea decizională şi războiul de manevră; superioritatea cunoştinţelor şi cunoştinţele despre război.

Succesul în războiul de manevră se obţine numai prin Superioritatea Cunoştinţelor.

Se tratează apoi problema Superiorităţii Informaţionale şi superiorităţii cunoştinţelor în războiul de manevră. Lucrare de referinţă: *Manevra decisivă*.

Succesul războiului de manevră presupune superioritatea cunoştinţelor utilizând superioritatea informaţională.

În continuare se tratează natura avantajului Cunoştinţelor şi relaţionarea cu avantajul Deciziei şi avantajul informaţiilor.

Decizia presupune cunoştinţe utilizând informaţiile.

Raportul se încheie cu o discuţie pe temele tratate şi cu câteva recomandări privind evoluţia viitoare a fenomenelor discutate.

Superioritatea Informaţională, cunoaşterea şi Network centric Warfare

Martin Burke,

1. Contextul

Toate argumentele legate de NCW şi avantajul Cunoaşterii prezentate aici utilizează concepte care vor fi dezvoltate pe parcursul raportului.

2. Fundamente ştiinţifice

Joint Vision 2010 care reprezintă *modelul conceptual pentru armata americană*. Se subliniază importanţa obţinerii cunoştinţelor privind câmpul de operaţii prin intermediul sistemelor de sisteme care utilizează sistemele tehnologice integrate.

„Ne trebuie Superioritatea Informaţională: capacitatea de a colecta, procesa şi disemina într-un flux continuu, neîntrerupt simultan cu exploatarea sau blocarea adversarului de a face acelaşi lucru.”

„Baza acestui cadru de lucru o regăsim în îmbunătăţirea funcţiilor de comandă-control şi a activităţii de intelligence care pot asigura superioritatea informaţională.”

Strategia Politică a Australiei (ASP97) stabileşte direcţiile pentru apărarea secolului 21. Ea explică de ce în războiul viitorului victoria se va obţine prin obţinerea, pe cât este posibil, a tuturor informaţiilor relevante despre adversar.

Se sublinia că avantajul Cunoaşterii (exploatarea eficientă a tehnologiilor informaţionale în scopul obţinerii

rezultatelor maxime cu minim de forţe), reprezintă cea mai înalta capacitate care trebuie dezvoltată prioritar.

Niciunul din cele două documente nu pun accentul pe Superioritatea Cunoştinţelor. Acest termen este utilizat în raport ca desemnând capacitatea de inducere în eroare a adversarului în scopul creări confuziei şi adoptării deciziilor greşite. De asemenea, niciunul din cele două documente nu pun accent pe factorul uman, purtător şi transmiţător de cunoştinţe şi informaţii. Ele pun accentul mai degrabă pe Superioritatea Informaţională asupra adversarului decât pe producerea confuziei în rândurile acestuia.

Situaţia poate fi interpretată ca un fenomen socio-cultural în care predomină alţi factori decât cei raţionali. Acest raport nu urmăreşte nicidecum o analiză a fenomenului socio-cultural. Această problemă a fost tratatată în lucrarea *Sisteme de gândire şi NCW* (Burke, 2000).

3. Obiective, abordare, structură

Raportul urmăreşte să aducă contraargumente ideii conform căreia „în războiul modern succesul poate fi asigurat prin Superioritate Informaţională”

Demonstraţia se va face pornind de la acele definiţii şi explicaţii din cele două lucrări descrise mai sus, JV2010 şi ASP97.

4. Superioritatea Informaţională, Superioritatea Cunoştinţelor şi NCW

În lucrarea Network Centric Warfare (Alberts, Garstka et al., 1999) s-a încercat demontarea ideii conform căreia „în războiul modern succesul poate fi asigurat prin Superioritate Informaţională”

NCW este definit ca: superioritate informaţională care duce la creşterea puterii combative prin senzorii din reţele, factori de decizie urmărind obţinerea punerii în comun a cunoştinţelor, creşterea vitezei de comandă şi a sincronizării forţelor. În esenţă Network Centric Warfare translatează Superioritatea Informaţională în putere de luptă prin eficientizarea legăturilor dintre entităţile din

câmpul de operaţii. Puterea Network Centric Warfare este derivată din eficienţa legăturilor din reţele sau punerea în reţele a entităţilor dispersate din punct de vedere geografic.

Superioritatea Informaţională este redefinită astfel: stare care este realizată atunci când avantajul competitiv este derivat din capacitatea de exploatare a poziţiei superioare din punct de vedere informaţional.

Această vedere revizuită este şi ea eronată. Avantajul competitiv în NCW nu presupune în mod necesar o superioritate informaţională în cazul în care un actor poate crea confuzie în rândurile adversarului fiind mai bine informat decât acesta.

Concluzie:

Succesul NCW presupune Superioritatea Cunoştinţelor utilizând Superioritatea Informaţională.

5. Superioritatea decizională şi războiul de manevră; Superioritatea Cunoştinţelor şi Războiul Informaţional.

În lucrarea *Manevra decisivă*(1998) acest concept este definii astfel: *conducerea sincronizată a operaţiilor folosind toate mijloacele mobile şi imobile din mediul respectiv în scopul atacării punctelor critice, vulnerabile ale adversarului puntru cucerirea punctului central şi obţinerea succesului maxim*.

Superioritatea Decizională este definită astfel: Decizia luată într-un anumit ritm astfel încât forţele säße capabile să utilizeze în mod superior cunoştinţele atât pentru sucesul propriu cât şi pentru a bloca accesul adversarului la astfel de informaţii despre forţele proprii.

Relaţia dintre superioritatea decizională şi războiul de manevră poate fi sintetizată astfel:

Războiul de manevră este războiul modern;

Războiul de manevră conţine războiul Informaţional (al cunoştinţelor);

Succesul în războiul de manevră presupune Superioritatea Decizională;

Succesul în Războiul Informaţional presupune Superioritatea Cunoştinţelor;

Superioritatea Decizională presupune Superioritatea Cunoştinţelor.

Concluzie:

Succesul în războiul de manevră se obţine numai prin Superioritatea Cunoştinţelor.

6. Superioritatea Informaţională, Superioritatea cunoştinţelor şi războiul de manevră.

În aceeaşi lucrare, Manevra decisivă (1998), se clarifică relaţia dintre Superioritatea Informaţională şi Superioritatea Decizională: Conflictul reprezintă un proces dinamic în care rezultatele acţiunilor planificate nu pot fi complet predictibile. Chiar şi în cazul celui mai bun plan nu putem ieşi complet teferi din conflictul cu un adversar. Pentru a fi eficientă manevra decisivă trebuie să se bazeze pe monitorizarea continuă a situaţiei pentru a fi capabili să reacţionăm mult mai repede decât adversarul. Aceasta se obţine prin Superioritatea Decizională, dezvoltată prinţi-un management informaţional superior şi asigurat de o stare robustă de securitate.

Aspectele relevante sunt următoarele:

Succesul războiului de manevră presupune Superioritate Decizională;

Succesul războiului de manevră utilizează Superioritatea Informaţională.

Concluzie:

Succesul războiului de manevră presupune superioritatea cunoştinţelor utilizând superioritatea informaţională.

7. Decizia, Cunoştinţele şi Informaţiile în orice conflict unul dintre adversari beneficiază de superioritate. În mod particular, în războiul de manevră:

Avantajul decizional există doar la cel care beneficiază de superioritate asupra celuilalt.

În Războiul Cunoştinţelor avantajul cunoştinţelor există doar la cel care beneficiază de Superioritatea Cunoştinţelor asupra celuilalt.

În războiul Informaţional avantajul informaţional există la cel care beneficiază de superioritate

Informaţională asupra celuilalt.

Avantajul decizional presupune avantajul Cunoştinţelor utilizând avantajul Informaţiilor.

Această aserţiune poate fi întărită printr-un citat din lucrarea *Manevră decisivă*:

Pentru ca Inovaţia să aibă efectele dorite trebuie să se bazeze atât pe cunoaşterea comprehensivă a punctelor tari, punctelor slabe şi intenţiile ale adversarului cât şi pe cele proprii. Desfăşurarea oricărei acţiuni trebuie să se bazeze pe cunoaşterea detaliată a mediului strategic şi tactic pentru a diminua posibilitatea apariţiei efectelor nedorite.

Mai departe se subliniază faptul că există diferenţe profunde între natura corpului cunoştinţelor şi forţele militare. O trăsătură necesară obţinerii şi menţinerii avantajului cunoştinţelor va fi înţelegerea potenţialului inamicului şi a felului în care acesta este exploatat.

De asemenea, trebuie să înţelegem că superioritatea cunoştinţelor asupra unui inamic nu înseamna superioritate şi asupra altui inamic. Acesta este un concept relativ.

După cum trebuie să înţelegem că este totodată şi un concept dinamic, care suportă schimbări rapide în urma interacţiunilor sistemului cu presiuni noi.

8. Discuţii şi concluzii

Raportul a supus observaţiei auditoriului apariţia unui nou fenomen socio-cultural în comunitatea Apărării care porneşte de la ideea că „în războiul modern succesul poate fi asigurat prin Superioritate Informaţională”. Pe tot parcursul raportului au fost prezentate argumente în scopul demontării acestei aserţiuni care tinde să fie generalizată.

Concluziile la care s-a ajuns în urma discuţiilor sunt următoarele:

În NCW succesul presupune Superioritatea Cunoştinţelor utilizând Superioritatea Informaţională;

Succesul războiului de manevră presupune superioritatea cunoştinţelor utilizând superioritatea

informaţională;

Avantajul decizional presupune Avantajul Cunoştinţelor utilizând Avantajul Informaţiilor.

Totuşi trebuie să amintim că acest raţionament nu este complet riguros dar este plauzibil având în vedere că se bazează pe două surse doctrinare: JV2010 şi ASP97. Apărarea militară nu trebuie privită ca un fenomen static şi stabil care poate fi înţeles sau perfect realizabil, ci ca un fenomen dinamic, volatil şi eluziv. De aceea sunt necesare metode noi, diferite de cele adoptate până acum pentru a analiza şi gestiona acest fenomen. Este neceasară învăţarea şi aplicarea acestor metode specifice războiului viitorului.

Războiul Informaţional şi Războiul Cunoştinţelor

Această anexă prezintă două fragmente de referinţă din lucrarea lui Philippe Baumaid,

De la Războiul Informaţional la Războiul Cunoştinţelor (1996).

„Există iluzia că dezvoltarea unei structuri informaţionale este o condiţic necesară şi suficientă pentru a dobândi infrastructura naţională a cunoştinţelor. Din contră, o astfel de politică se dovedeşte contraproductivă. Ea va conduce la separarea corpului cunoştinţelor de la cele mai înalte nivele care se va rupe de realităţile sociale cotidiene şi, în cele din urmă la crearea unei nişe între oamenii care acţionează, învaţă, vorbesc şi oameni care au acţionat, au învăţat, au vorbit.”

„Wilenski spunea că „informaţia a fost o sursă de putere iar azi a devenit o sursă de confuzie”. În fiecare sferă a vieţii modeme s-a produs o suprasaturare cu informaţie, care a dus de cele mai multe ori la pierderea sau integrarea deficientă în sistem. Rădăcinile acestei probleme sunt următoarele:

(a) confuzia persistentă dintre informaţii şi cunoştinţe,

(b) concentrarea sistemului educaţional actual pe acumularea de cunoştinţe de bază vs. Îmbunătăţirea diversităţii şi flexibilităţii modelelor de gândire,

(c) eşecul introducerii în entităţile organizaţionale a ideilor novatoare. Managerii sunt conştienţi că fenomenul adaptabilităţii este o asigurare în găsirea celor mai eficiente soluţii pentru rezolvarea problemelor organizaţionale. Cu toate că există o percepţie destul de consistentă asupra cunoaşterii, predomina distincţia netă între conceptul de,,organizaţie" şi cel de „cunoştinţe/cunoaştere"

Specialiştii în teoria organizaţiilor au propus o serie de soluţii alternative originale care pun accentul pe socializare şi participarea colectivă la construcţia organizaţională şi la generarea cunoştinţelor"

Kasparov vs. Kasparov

Această anexă cuprinde un studiu de caz care să ilustreze dependenţa de informaţie în timpul unui conflict. Kasparov este un jucător de şah fanatic. A studiat multe cărţi de şah şi a analizat multe partide istorice.

Fiul său Gary a fost învăţat de mama sa să joace şah la o vârstă foarte timpurie. La 4 ani a bătut-o la şah pe mama sa pentru prima dată.

Kasparov tatăl, evident, avea mai multă experienţă şahistică decât fiul său. Fiul nu a avut acces la informaţia la care nici mama nu a avut acces, în ciuda acestui dezavantaj talentul său precoce i-a permis să îşi dezvolte cunoştinţele despre modalităţile de joc, etc. Astfel a întrecut-o pe mama sa.

Acest exemplu ne demonstrează că superioritatea informaţională nu este de ajuns pentru a câştiga într-un conflict de cunoştinţe.

Învatamintele acestei istorioare sunt:

Ambii jucători aveau informaţii complete şi identice;

Kasparov tatăl avea mai multe informaţii decât fiul său;

Gary Kasparov nu a dispus de informaţia relevantă de care nu dispunea nici mama sa.

Rezultă că superioritatea informaţională nu este necesară pentru superioritatea cunoştinţelor. Cazul ne demonstrează că în anumite circumstanţe abilitatea de a

învăţa şi de a aplica aceste cunoştinţe este mult mai importantă decât accesul la o multitudine de informaţii relevante. Aici există mai mulţi factori explicativi:

Informaţia codificată din ADN pe care mama a partajat-o cu fiul;

Informaţiile din creierul jucătorilor rezultate în urma observării jocului;

Informaţiile din cărţile de şah pe care Kasparov tatăl le-a citit şi le-a interpretat;

Informaţiile transmise de la mamă la fiu pe parcursul învăţării şi antrenării.

Cele 7 „păcate” ale NCW

Th. Barnett

Cei mai mulţi dintre noi au citit articolul vice-amiralului Art Cebrowski din 1998 despre NCW şi au putut vedea viziunea oarecum îndrazneata care era prezentată acolo. Pornind de la citatul lui Lidell-Hart „mai greu decât pătrunderea unei idei noi în armată este renunţarea la ideea învechită”, Cebrowski şi coautorul A. Gartska aruncă mănuşa spre provocarea tuturor celor care le-ar putea dovedi că nu au dreptate absolută.

Autorul acestui articol urmăreşte să identifice şi să comenteze unele neajunsuri ale NCW, după cum le-a numit „păcate, dar, atenţie, nu păcate de moarte”.

PATIMA

NCW tânjeşte după un adversar cu putere tehnologică. Este îndoielnic că, din această perspectivă, SUA s-ar putea confrunta cu un adversar pe măsură. SUA cheltuiesc pe tehnologic informaţională mai mult decât ar cheltui două ţări cu întreaga armată.

În timp ce aliaţii SUA se străduiesc să ţină pasul cu americanii ne putem întreba în ce moment aceştia vor fi la fel de pregătiţi din acest punct de vedere? Într-o lume în care naţiunile cheltuiesc în medie 5 miliarde de dolari pentru Apărare, NCW reprezintă o cărare bătută doar de americani.

De aceea nici măcar aliaţii cei mai de seamă ai americanilor nu pot să ţină pasul cu această cursă a

„comunicării”

În continuare autorul ne vorbeşte despre manifestarea efectului QWERTY[114].

Acesta este clar monopolul americanilor, celelalte fiind doar simple copii mai mult sau mai puţin performante ale tehnologiei americane.

Să ne amintim momentul când Iranul a primit tehnologic pentru rachete de la Coreea de Nord. Aceasta reprezintă o copic săracă a tehnologiei chinezeşti, o copie şi mai săracă a tehnologiei sovietice, şi o copie şi mai săracă a tehnologiei naziste”

Iată de ce proliferarea rămâne mai lentă decât sugerează cei mai mulţi experţi în legătură cu NCW.

Dacă ţările competitoare se apropie cât de cât de performanţele tehnologice americane, ţările mici, inamice ale SUA, care îşi revendică drepturile evident nu pot fi considerate inamice din perspectiva NCW.

În aceste condiţii SUA ar trebui să îşi tempereze patima după adversari demni din perspectiva NCW.

NEPĂSAREA

Militarii americani se adaptează foarte lent la NCW în lumea „MOOTW” (operaţiile militare altele decât războiul). Acestui tip de operaţii trebuie să le facă faţă militarii americani azi.

De aceea se pune problema cum s-ar putea aplica NCW aici? Soldaţii să comunice între ei prin cabluri? Sau să comunice cu lumea exterioară?

Aceasta nu este o întrebare ezoterică pentru forţele navale deoarece va veni un moment când reţeaua informaţională va deveni crucială pentru marina americană în momentele de criză mai ales când predomină confuzia şi haosul. De aceea NCW trebuie să reprezinte o cale spre rezoluţie şi nu spre conflict. Forţele navale trebuie să reprezinte un „nod” conector, nu un nod distructiv.

---

114 De la computer, simbolurile primelor taste
" Nimic mai fals, şi tehnologia de rachete americană are ca sursă tehnologia de rachete nazistă (nota S.E.)

Dacă va fi folosit corect NCW va permite militarilor americani să intervină pentru rezolvarea oricărei situaţii de criză şi să instaleze o „umbrelă informaţională” care să facă reclamă transparenţei acţiunilor întreprinse.

ZGÂRCENIA

NCW promovează principiul „mult şi ieftin” în timp ce armata merge pe „puţin şi scump”. Mulţi experţi susţin, şi pe drept cuvânt, că NCW nu aduce nimic nou faţă de marină.

Marina americană reprezintă un mediu interconectat. În toate serviciile importante din acest departament avem de-a face cu conectare de tip NCW. Nu este niciun secret pentru nimeni că Marina a sacrificat un număr important de vase în favoarea achiziţiilor tehnologice.

Ceea ce ne face să estimăm că Marina va sărăci în viitoarea eră a NCW unde contează mobilitatea şi flexibilitatea. Pentru că şansele de confruntare cu inamici aflaţi în paradigma „puţin şi ieftin” sunt foarte mari. De aceea paradigma americană „mult şi scump” nu va mai fi funcţională.

MÂNDRIA

Strategiile de blocare specifice NCW vor duce la resuscitarea vechiului mit al bombardamentului strategic.

Până în 1921 (Giulio Douhet, *Comanda aerului*) se credea că o lovitură aplicată în centrul de greutate a inamicului conduce la o victorie rapidă fără victime.

Această paradigmă persistă şi azi în viziunea teoreticienilor NCW prin conceptul de „Blocare strategică”. Chiar dacă oponenţii NCW admit sau nu, cele două strategii au în comun ideea falsă că pedeapsa înseamnă control. Distrugând tehnologia informaţională a inamicului, înseamnă că îl anihilăm?

Nu. De ce?

În primul rând pentru ca RI desfăşurat de o ţară reprezintă terorism internaţional desfăşurat de o altă ţară. Dacă o putere ostilă ar încerca să deformeze scopurile noastre am fi acuzaţi de tot felul de crime de război.

Pagubele colaterale asociate decapitării tehnologiei

informaţionale sunt prea complexe pentru a fi controlate de la distanţă.

În al doilea rând structurile responsabile cu evaluarea pagubelor produse de bombardamente sunt azi capabile să măsoare şi efectele în masă ale NCW. Unii presupun ca micşorarea gradului de tehnologizare informaţională a societăţilor mici determină creşterea abilităţii americane de a înţelege impactul războiului informaţional.

În al treilea rând, în timp ce salută această teorie complexă, cel care promovează conceptul de NCW renunţă la tot ceea ce înseamna blocare strategică.

În al patrulea rând NCW este vinovat de «imagine în oglindă”: noi teoretizăm despre vulnerabilităţile tehnologiei noastre informaţionale şi presupunem, totodată că şi alţii fac acelaşi lucru.

FURIA

Presupunerile privind creşterea vitezei de comandă sunt generate de faptul că date şi informaţii ne parvin cu viteză foarte mare. Acest cerc virtuos se poate transforma într-unui vicios dacă entităţile decizionale vor deveni sclave ale computerelor lor.

Rapiditatea cu care pot circula deciziile greşite, iată adevăratul pericol. Şi mai îngrijorătoare sunt presupunerile privind intruziunea în mecanismul decizional al inamicului. Aceasta a devenit un scop cu toate că ar trebui să ne centrăm pe ceea ce trebuie să facem în momentul în care pătrundem acolo.

Vorbim mereu despre potenţialul inamicului cu tehnologie informaţională mai puţin dezvoltată, ceea ce face ca percepţia deformată să fie uriaşă.

INVIDIA

NCW râvneşte spre sincronizarea cu lumea comercială a afacerilor. Nicio armată din lume nu este mai armonizată decât cea americană.

În nicio armată nu se urmăreşte scopul descentralizării deciziei ca în aceasta. Deci dacă vreo armată se va adapta la NCW prin realizarea principiului

sincronizării, aceasta va fi cea americană. Scopul auto-sincronizării este acela că tehnologia informaţională va facilita o transmitere extrem de rapidă a informaţiei permiţând comandanţilor să exploateze la maximum viteza de comandă. Invidia NCW faţă de lumea afacerilor din perspectiva sincronizării cu piaţa este o atitudine pe care o putem înţelege.

Aceasta deoarece operaţiile militare sunt poate faptele cele mai complexe din lume. Dar această invidie este prost plasată. Sunt create guverne care să rezolve problemele spinoase ale societăţii pe care credem că firmele particulare nu le pot gestiona sub motivaţia că scopul lor ultim este acela de a obţine profit. Şi, printre aceste probleme spinoase sunt şi cele militare.

LĂCOMIA

Termenul „tablou comun al câmpului de operaţii" din viziunea teoreticienilor NCW desemnează faptul că toţi actorii din câmpul de operaţii trebuie să îmbrăţişeze acelaşi model mintal. Nfe îndoim că numai prin intermediul prezentărilor multi-media se vor putea pune în comun informaţiile despre realităţile câmpului de luptă.

Noutatea este reprezentată de capacitatea rapidă de inundare cu informaţii. În cazul în care acestea sunt eronate percepţia eronată se poate generaliza iar deciziile adoptate vor fi evident greşite.

Ambiţia NCW devine cu atât mai îngrijorătoare cu cât există fenomenul de filtrare la transmiterea informaţiilor de la un nivel la altul de comandă. NCW promite să netezească ierarhiile, dar natura complexă şi gravă a operaţiilor militare poate împinge mai mulţi comandanţi la adoptarea unor decizii fanteziste.

Infuzia tehnologiilor informaţionale în organizaţiile ierarhizate reduce asimetriile tradiţionale conform cărora doar entităţile din vârful piramidei beneficiau de informaţii complete. Din această perspectivă conceptul de „tablou comun al câmpului de operaţii" este o încercare de a limita prerogativele şi tendinţele exclusiviste ale înalţilor comandanţi militari.

Tentaţia lăcomiei faţă de informaţii va exista întotdeauna la NCW.

CONCLUZIE

Aici nu s-a încercat nici să se discrediteze conceptul de NCW nici negarea sa. Trecerea în viitor a structurilor Apărării la paradigma NCW va fi inevitabilă.

Viitorul este al RĂZBOIULUI în REŢEA.

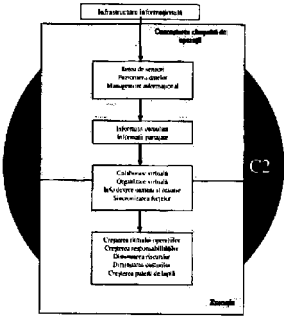


Figura î – Infrastructura informaţională

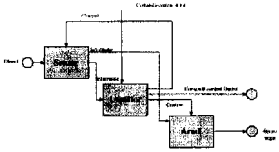


Figura 2 – Componentele funcţionale ale angajării unui luptător comandând o „forţă” în teren

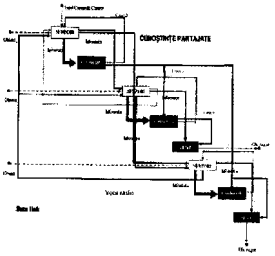


Figura 3 – Nivele de cunoaştere ale cunoştinţelor partajate

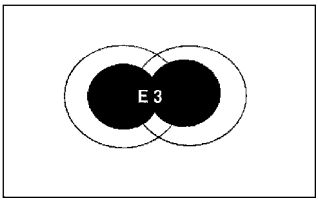


Figura 4 – Platform Centric Engagement Envelope

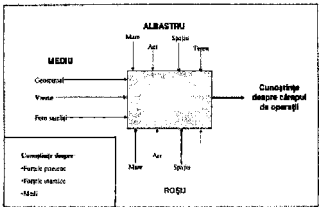


Figura 5 – Cunoaşterea câmpului de luptă

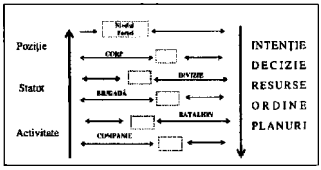


Figura 6 – Partajarea informaţiilor pe eşaloane şi ierarhii

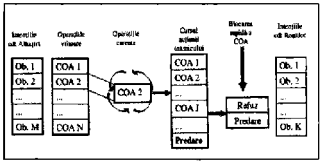


Figura 7 – Conceptul de blocare strategică

ANEXA 2

1. RĂZBOIUL INFORMAŢIILOR A DEVENIT DEJA O REALITATE A CÂMPULUI DE LUPTĂ MODERN

Evoluţia tehnico-ştiinţifică contemporană extrem de spectaculoasă, se răsfrânge într-o măsură pregnantă atât asupra evoluţiei societăţii, cât şi asupra dezvoltării organismului militar sub toate aspectele.

În câmpul de luptă modem, influenţa informaţiilor devine hotărâtoare, cu însemnate repercursiuni asupra eficacităţii armamentului şi moralului luptătorilor şi, în

consecinţă asupra deznodământului luptei. În societatea informaţională, în contextul creşterii explozive a utilizării informaticii, comunicaţiilor şi mijioacelor de luptă cibemetizate, informaţia devine obiectivul, mijiocul şi procedura unei noi forme de război – războiul informaţiilor.

Pentru acest tip de război nu sunt încă definiţii oficiale. O definiţie acceptată de mai mulţi specialişti a fost cea formulată de dr. John Alger de la Universitatea „George Washington" ca reprezentând: „acţiunile întreprinse pentru a asigura superioritatea informaţională prin afectarea informaţiilor, proceselor de prelucrare şi a sistemelor informatice ale inamicului concomitent cu apărarea celor proprii.

O altă definiţie a fost emisă de ministrul apărării al S.U.A.: „acţiunile întreprinse pentru asigurarea superiorităţii informaţionale în sprijinul strategiei militare naţionale prin afectarea informaţiilor şi sistemelor informaţionale ale adversarului, concomitent cu apărarea şi utilizarea în siguranţă a sistemelor informaţionale proprii".

După aprecierea majorităţii specialiştilor care au abordat războiul informaţional, acesta ar viza cele două componente de bază (hardware şisoftware) utilizate în:

— sistemele de comunicaţii;

sistemele de calculatoare (reţele calculatoare, poştă electronică, etc.);

— sistemele de conducere şi dirijare a tehnicii de luptă şi armamentului;

sistemele de război electronic (în general de bruiaj electronic);

— sistemele de război psihologic (în special dezinformarea). Războiul informaţional poate fi:

— de apărare (cuprinzând măsurile de protecţie a sistemelor informaţionale proprii);

— Ofensiv (cuprinzând acţiunile de neutralizare a sistemelor informaţionale ale adversarilor);

Războiul informaţional vizează:

— controlul deciziilor şi al modului de elaborare al

acestora;

— paralizarea funcţionărilor structurilor organizatorice şi a relaţiilor dintre acestea;

— influenţarea proceselor decizionale;

— structurile decizionale ale domeniului politic, economic, social şi militar";

— blocarea fluxului informaţional dintre factorii politici de conducere şi organismul militar, dintre structurile politice şi celc administrative, dintre structurile civile şi cele militare, dintre conducere şi luptătorul (executantul) propriu-zis;

— controlul general sau parţial asupra mass-media pentru denaturarea realităţii, şi micşorarea oportunităţii informării, generarea confuziei şi a neîncrederii în structurile politico-militarc, în comandanţi;

— crearea unei false atmosfere de nelinişte ori de prea mare încredere;

— manipularea informaţională a comandanţilor, populaţiei şi a luptătorilor;

— deturnarea sau anihilarea funcţionării armelor inteligente şi a sistemelor de conducere ale acestora"

— generarea şi gestionarea crizelor informaţionale.

Eficacitatea acţiunilor de luptă informaţională este cu al Ai mai mare eu cât este mai intensă, iar mijioacele de securitate ale adversarului sunt mai puţin performante.

Războiul informaţiilor se poartă în toate mediile de ducere a războiului energetic şi este dublat de un război electronic generalizat, astfel încât nimic nu începe, nu se desfăşoară şi nu se termină fără informaţii şi contrainformaţii, fără prelucrări, procesări şi transmiteri. Războiul informaţiilor se poartă atât la vedere, cât şi, mai ales în ascuns, cu mijloace şi sisteme sofisticate, cu acţiune imediată sau cu efecte întârziate.

Perioadele cele mai acute ale războiului informaţional sunt cele de criză în care abundă situaţiile haotice, se diminuează capacităţile de orientare, se micşorează libertatea de acţiune, se măreşte responsabilitatea deciziilor şi se amplifică sentimentul de

nesiguranţă. De fapt, situaţiile de criză constituie, pentru sistemele informaţionale, adevăratele situaţii de test, în care tot ceea ce reprezintă neutilitate se accentuează, iar ceea ce înseamnă slăbiciune poate deveni catastrofală.

Forţele care poartă acest război:

— efectivele de luptă electronică specializate, care dispun de mijloace şi posibilităţi deosebite, ce pot acţiona direct în câmpul de luptă, precum şi în mediile complementare;

— forţele de cercetare -diversiune, dotate cu mijloace mobile rapide şi electronice performante de ultimă generaţie;

sistemele de armament care includ şi o componentă electronică (arme inteligente);

— ”teroriştii informaţionali”, organizaţi sau pe cont propriu (izolaţi);

— spioni în slujba unor state sau organizaţii internaţionale (structuri de informaţii ofensive);

— ”hacker-îi” (spărgătorii de coduri şi sisteme de securitate informaţională de acţiune pe cont propriu, pentru plăcerea de a „demola” barierele oficiale şi de a-şi încerca forţele, dar care pot fi manipulaţi şi utilizaţi, fără ştiinţa lor, de tot felul de organizaţii teroriste);

„curioşii”, utilizatori de sisteme şi mijioace informatice conectaţi la sistemele interne sau internaţionale şi care iscodesc, compară, analizează; schimbă şi actualizează de dragul surprizei; aceştia deşi în aparenţă inofensivi pot produce efecte considerabile, chiar catastrofale, dar pot fi şi manipulaţi;,

— Amatorii de senzaţii tari neinstruiţi, neavizaţi, care, jucându-se cu calculatorul pot produce necazuri mari;

— sisteme inteligente, special destinate acestui scop şi viruşimarea nenorocire a epocii informaţionale”.

Niciunul din aceste atacuri nu trebuie subevaluat, fiecare fiind susceptibil de a produce pagube imense sau catastrofale economice, politice ori militare.

Multe din aceste activităţi sunt calificate de către

specialişti drept crimă împotriva umanităţii.

În urma concluziilor desprinse din acţiunile de război informaţional şi din studiile întreprinse, armata americană a élaborât o nouă concepţie de contracarare a efectelor războiului electronic sintetizată în câteva direcţii de acţiune (10):

— asigurarea luptătorului cu sisteme specifice câmpului de luptă modern;

— Optimizarea mijloacelor privind tehnologia informaţională;

— implementarea securităţii informaţionale la toate nivelele (acoperire prin criptare şi alte metode);

— asigurarea supremaţiei electromagnetice şi utilizarea modului/TEMPEST-*

— utilizarea modelării şi simulării în pregătire etc.

Principiile informaţiilor a) Suficienţă informativă – principiul similar cu cel al suficienţei de resurse energetice, financiare, etc.) are în vedere satisfacerea, în condiţii de oportunitate a necesarului de informaţii atât pentru conducerea acţiunilor de luptă (în folosul statelor majore), cât şi pentru executarea misiunilor de către sistemele de armament sau chiar de luptători individuali.

Suficienţa informaţiei reprezintă un principiu de echilibru stabilit în funcţie de riscul operativ asumat şi costul posibil de suportat şi determinat de:

— cantitatea şi distribuţia pe domenii a informaţiei;

— capacitatea de procesare, prelucrare tactic-operativă şi de transmitere a informaţiei;

— ritmul actualizărilor şi schimbărilor pe care le generează sau împiedică schimbul de date.

Între suficient şi optim există o relaţie dinamică, fiind o valoare în jurul căreia oscilează suficientul.

Pericolele ignorării principiului suficienţei informaţiei sunt:

— subevaluarea – care determina lipsa de informaţii şi deci o decizie insuficient documentată şi susţinută informativ;

— supraevaluarea – deci o cantitate mai mare a

informaţiilor decât cea necesară ceea ce ducc la suprasaturarea informativă, îngreunarea selecţiei informaţiilor utile, întârziere în procesare şi transmitere, care afectează operativitatea în elaborarea variantelor şi soluţiilor optime şi, deci, întârzierea elaborării şi aplicării hotărârii.

b) Proporţionalitatea distribuţiei – principiul similar cu cel al structurii proporţionale a forţelor necesare ducerii războiului şi are în vedere distribuţia, în funcţie de necesităţi şi zone de interes ierarhizat, a fluxului de informaţii pe problematicile conducerii, execuţiei şi pe capacitatea de procesare şi transmitere.

Acest principiu este suficient atunci când pentru fiecare domeniu în parte sau misiune se asigură o suficicnţă informativă, fără goluri mari sau vârfuri însemnate de informare.

Proporţionalitatea distribuţiei informaţiilor este rezultatul unei activităţi profesionale deosebite şi trebuie satisfacută de dinamica acţiunilor de luptă, atât pe timpul elaborării hotărârii cât şi pe timpul executant misiunilor, având în vedere că realităţile informative se schimbă foarte des, schimbarea nu este liniară, fiind greu de prevăzut şi contracarat.

c) Oportunitatea informării – principiul cel mai invocat de analiştii militari, ce derivă din Oportunitatea hotărârilor şi a operaţiilor şi are în vedere culegerea de informaţii în timp operativ -real, cât şi procesarea şi transmiterea acestora la mediile cu necesităţi de informare.

Oportunitatea informaţiei are deci două componente (caracteristici):

— caracteristica temporaldinamică;

— componenta dependentă de cantitatea de informaţii necesarc de calitatea şi credibilitatea acestora, de capacitatea de procesarc şi transmitere.

d) Credibilitatea informaţiilor – cel mai vechi principiu, carc pune în raport cantitatea de informaţii cu gradul de adevăr conţinui.

Complexitatea principiului derivă din dimensionalitatea sa, care se referă la:

— credibilitatea surselor de informaţii interceptate;

— abilitatea şi profesionalismul celor care interceptează sursele;

— siguranţa transportului informaţiilor (ne alterabile în timp);

— capacitatea de prelucrare şi desprindere a adevărului;

— discernământul celor informaţi.

Experienţa demonstrează că, nici după foarte mult timp, credibilitatea unei informaţii nu poate fi determinată şi garantată.

e) Accesibilitatea informaţiilor – este principiul cu valenţe deosebite, astăzi în epoca informatizării şi războiului cibernetic, însemnând capacitatea informaţiilor de a se exprima direct şi fără dubii prin semantica şi modul lor de reprezentare.

Informaţia cea mai accesibilă este informaţia cu semantica definită, explicit, fără ambiguităţi, într-un limbaj adecvai destinatarului sau utilizatorului cu un anumit nivel de pregătire şi grad de inteligenţă.

2. CARACTERISTICI ALE DINAMICII RESURSELOR INFORMAŢIONALE

— sporirea considerabilă a volumului informaţiilor necesare elaborant hotărârii şi ducerii acţiunilor de luptă (de 4-10 ori faţă de volumul informaţiilor vehiculate în cel de al doilea război mondial);

— creşterea posibilităţilor de informare, prin diferite mijioace de culegere (interceptare radio, radiaţii electromagnetice, reţele, calculatoare, poştă electronică, etc.);

— sporirea necesităţilor şi posibilităţilor de procesare şi de sinteză logică, atât în sfera conducerii cât şi în cea a execuţiei;

— influenţa fastă a procesării informaţiilor asupra eficacităţii sistemelor de armament dar şi cea nefastă a informaţiilor de disimulare a viruşilor calculatoarelor

asupra proceselor de execuţie specializate;

— creşterea explozivă a cantităţii de informaţii necesare luptătorului pentru a face faţă solicitărilor şi vitregiilor câmpului de luptă modem;

— raportul de 9-13 la 1 între acţiunile de război informaţional şi cele de lovire efectivă;

— apariţia, integrarea şi utilizarea armelor de luptă inteligentă (roboţi militari);

— apariţia şi perfecţionarea structurilor specializate de securitate a informaţiilor;

legătura indisolubilă dintre moral şi informare, dintre angajare şi cunoaştere, dintre acţiunea profesionistă şi realitatea câmpului de luptă;

— caracterul cibernetic al acţiunilor de luptă şi apropierea informaţională şi tehnologică dintre conducere şi execuţie.

Structurile de informaţii militare este necesar să-şi reconsidere unele elemente din Planul de căutare a informaţiilor. Mă refer la faptul că ele urmează să-şi pregătească componenta contrainformativă la asemenea parametri încât să fie capabili să facă faţă terorismului informaţional. Aceasta reprezintă de fapt o utilizare abuzivă a sistemelor informative digitale, reţelelor sau altor componente pentru un rezultat final care sprijină sau facilitează o acţiune sau campanie teroristă. În momentul când infrastructura informaţională va fi încheiată în armata noastră, ne putem aştepta oricând la acţiuni de acest gen.

Considerând că deocamdată, armata română se găseşte încă departe de riscurile unor asemenea ameninţări plecând în special de la premisa inexistenţei unei infrastructuri generale adecvate, dar asemenea ameninţări pot ajuta mult la pregătirea unor măsuri de protecţie pentru cazul în care vom fi în măsură şi vom avea ceva de apărat în acest domeniu.

3. OPERAŢIILE INFORMAŢIONALE

„în secolul XXI, operaţiile se vor baza foarte mult pe cunoaşterea rezultată din date şi informaţii relevante

culese, prelucrate, analizate şi difuzate printr-un sistem global complex de sisteme. Acest cadru evolutiv de informare militară va schimba fundamental modul de desfăşurare a operaţiilor de către trupele de uscat în timp de pace şi în conflicte... Trupele de uscat vor integra operaţiile informaţionale în fiecare aspect al concepţiei Trupele de Uscat XXI.

Folosind avantajele operaţiilor informaţionale, comandanţii trebuie să fie conştienţi că bizuirea trupelor de uscat pe tehnologiile de informare creează noi vulnerabilităţi şi cursuri de acţiune asimetrice, avantajoase pentru inamic. Conceptul superiorităţii informative se bazează pe disponibilitatea de informaţie. De aceea, informaţiile şi sistemele de informare (INFOSYS) trebuie protejate. Operaţiile informaţionale se desfăşoară într-un „cadru naţional total care adaptează mijloacele la obţinerea superiorităţii militare (ca şi a celei diplomatice şi economice) asupra adversarului pe baza cunoaşterii...,,. Aceste concepte privind operaţiile informaţionale duc spre noi modalităţi de a gândi războiul, spre responsabilităţi noi şi chiar spre noi relaţii pentru comandanţi.

Provocările la care trebuie să facă faţă trupele de uscat sunt tot atât de dinamice ca şi lumea în care trăim. Schimbările rapide aduse de cipurile de calculator şi de progresele din domeniul telecomunicaţiilor au afectat profund mediul nostru. Lumea este acum interconectată şi interactivă. Mediul global informaţional (GIE) evoluează zi de zi. Împreună cu progresul ştiinţei şi cu forţa calculatoarelor, GIE aduce avantaje enorme umanităţii în domenii ca: medicina, educaţia şi industria. Acest mediu promite mult dar prezintă şi noi sfidări, vulnerabilităţi şi ameninţări. În interiorul său nu există hotare politice sau teritoriale, ceea ce face ca „actele de război „ să capete caracter ambiguu.

Componentele întregii infrastructuri americane – finanţe, energie, educaţie, transporturi, telecomunicaţii, apărare şi majoritatea aspectelor societăţii sunt legate între ele şi interdependente. Departamentul Apărării se

bazează pe reţelele comerciale de telecomunicaţii pentru mai mult de 95% din traficul său de informaţii. Acest lucru face SUA, în calitatea lor de principală ţară a lumii, dependente de tehnologie, mai sensibile decât oricare alt stat la acţiuni adverse. Chiar şi în cazul unui inamic slab, operaţiile informaţionale oferă un profit disproporţionat de mare pentru orice investiţie.

Progresul tehnologie nu face ca lumea să fie mai sigură şi mai liniştită. Creşterea alarmantă a conflictelor regionale a dus la intensificarea tensiunilor şi a făcut lumea mai complexă şi mai instabilă. În plus, fanatismul unor secte continuă să producă destabilizare în întreaga lume Terorismul este mai sofisticat şi ar putea implica folosirea unor arme de nimicire în masă şi atacarea reţelelor de calculatoare şi sistemelor care controlează reţeaua energetică naţională, traficul aerian şi alte infrastructuri importante. Chiar şi un adversar mai puţin sofisticat care are foarte puţini bani poate obţine sau chiar închiria o gamă largă de capacităţi în orice loc din lume. Tehnologii precum sistemul de poziţionare globală (GPS), supravegherea prin sateliţi, comunicaţiile prin fibre optice, sistemele de emisie în direct, accesul la INTERNET, criptografia, sesizoarele şi armele de precizie sunt cu toate disponibile în comerţ. La preocupările legate de securitate se adaugă natura de sursă deschisă a GIE şi faptul că ne bazăm pe acest mediu. Adversari potenţiali ar putea obţine acces la date importante şi ar putea folosi mediul global informaţional pentru a ne ataca.

În această lume a comunicaţiilor globale, a sateliţilor, a imaginilor luate de sus şi a CNN, indivizii din orice colţ al lumii primesc informaţiile aproape instantaneu. Aceste informaţii şi relatări de presă afectează opinia naţională şi mondială, modelează acţiunile politicienilor şi produc o contopire a nivelului tactic, operativ şi strategie al războiului. Progresul tehnologic, relatarea informaţiilor în mass-media şi comprimarea relaţiilor timp-spaţiu contribuie la amplificarea raporturilor dintre nivelurile războiului, care îi ajută pe comandanţi să vizualizeze fluxul

logic al operaţiilor, să aloce resursele şi să încredinţeze misiunile celui mai potrivit comandament. Totuşi, comandanţii de la toate nivelurile trebuie să fie conştienţi că, într-o lume a comunicaţiilor directe, orice eveniment izolat poate să treacă prin toate cele trei niveluri. Relatările mass-media de astăzi ne măresc sensibilitatea atât faţă de pierderile proprii, cât şi faţă de cele ale inamicului. Operaţia de capturare a dictatorului militar somalez Mohamed Farah Aidid din 03.10.1993 este un exemplu clar de contopire a celor trei niveluri de război. Imaginea de televiziune cu trupul unui soldai american târât pe străzile din Mogadiscio a produs aproape imedial o schimbare a politicii naţionale. În acest caz a fost vorba de o misiune operativă, desfăşurată într-un cadru tactic, cu ramificaţii strategice.

3.1. Tehnologia şi dominaţia informaţională

Valorificând inovaţiile tehnologice, trupele constituie în prezent o forţă de luptă bazată pe informaţie.Tehnologiile de informare îi pot oferi comandantului o înţelegere clară a situaţiei sale curente în raport cu inamicul şi cu mediul. Printr-o prelucrarc deliberată şi sistematică a volumului mare de date, se obţin informaţii care, sintetizate într-un tot coerent, asigură cunoaşterea. Aceasta este cheia spre dominaţia informaţională, un grad de superioritate informaţională ce le permite comandanţilor să folosească INFOS YS şi posibilităţile la dispoziţie pentru obţinerea avantajului operaţional în lupta sau pentru controlarea situaţiei în alte operaţii decât cele de război.

Ţelul final al operaţiei informaţionale este de a-i face pe comandanţii de unităţi apţi să realizeze stăpânirea informaţiilor, interzicând acelaşi lucru inamicului. Comandanţii dobândesc această dominaţie informaţională când cunoaşterea situaţiei proprii, a mediului şi a inamicului potenţial le oferă un avantaj distinct. Eforturile de informatizare a trupelor de uscat vor sprijini acest proces printr-o cunoaştere mai bună a situaţiilor şi prin vizualizarea câmpului de luptă, influenţând profund

conducerca luptei şi desfăşurarea tuturor operaţiilor.

Dezvoltarea sistemelor de informare amplifică capacităţile comenzii şi controlului (C2) şi eficienţa armamentului. Avantajul tehnologic de care ne bucurăm a îmbunătăţit capacitatea de proiectare a forţelor şi de sprijinire a acestora în operaţiile executate la mare distanţă. Prin concepte ca „logistică la timp" „adunare de la distanţă" şi „vizibilitate totală a dispozitivului", vom face ca să fie mai eficiente şi să se poată susţine. Toate aceste eforturi, exemplificate de iniţiativa „Forţa XXI" a armatei americane, se bazează în principal pe capacitatea de a valorifica o multitudine de noi sisteme de informare. Totuşi sistemele sunt ameninţate de aceleaşi vulnerabilităţi de care suferă sistemele civile când o organizaţie devine dependentă total de tehnologie. Vulnerabilităţile sunt exacerbate şi de legătura acestora cu infrastructura civilă, şi de faptul că se bazează pe aceasta.

3.2. Teoria informaţiei informaţionale

Operaţiile informaţionale constau din „operaţii militare continue în mediul militar informaţional (MIE) care permit, întăresc şi protejează capacitatea forţelor proprii de a culege, prelucra şi folosi informaţiile pentru a obţine avantaje în toată gama de operaţii militare; operaţiile informaţionale includ interacţiunea cu mediul global informaţional şi exploatarea informaţiilor inamicului şi a capacităţilor sale de decizie sau interzicerea acestora".

Operaţiile informaţionale cuprind trei componente: operaţiile; sistemele de informare; cercetarea, obţinerea de date şi culegerea de informaţii (RII).

Operaţiile. Dimensiunea operaţii a operaţiilor informaţionale este compusă din toate măsurile, atât ofensive (atacarea C2) cât şi defensive (protecţia C2), folosite pentru obţinerea dominaţiei informaţionale. Pe câmpul de luptă, aceste acţiuni sunt numite cu termenul de luptă în domeniul comenzii şi controlului (C2W). comandanţii sincronizează elementele de luptă electronică (EW), măsurile de inducere în eroare a inamicului pe câmpul de luptă, operaţiile de securitate (OPSEC),

operaţiile psihologice (PS YOP) şi, dacă este necesar, distrugerea fizică şi le concentrează împotriva sistemelor C2 ale inamicului, personalului şi materialelor, precum şi asupra voinţei şi sprijinului populaţiei adverse. În acelaşi timp, comandanţii trebuie să-şi protejeze sistemele C2 proprii de atacurile inamicului sau de exploatarea acestora de către inamic.

În timpul desfăşurării operaţiilor, afacerile publice (PA) şi afacerile civile (CA) au un impact direct asupra operaţiilor informaţionale. Un plan coordonat de operaţie informaţională care încorporează afacerile publice şi afacerile civile este important pentru făurirea legitimităţii pentru naţiunea-gazdă, pentru coaliţie, pentru SUA şi pentru sprijinul mondial, în special în alte operaţii decât cele de război. Afacerile publice trebuie integrate în operaţiile informaţionale pentru realizarea unei informări corecte, echilibrate şi credibile. Activităţile de afaceri civile sunt importante pentru că realizează interfaţa cu organizaţiile şi cu indivizii importanţi din mediul de informare. În fine, consilierii juridici analizează legislaţia internaţională şi internă şi ajută la formularea unor reguli de angajare a operaţiilor informaţionale corespunzătoare conducerii desfăşurării operaţiilor.

INFOS YS. În mediul informaţional actual, comandanţii au nevoie de sisteme de informare robuste şi de încredere pentru culegerea, prelucrarea şi difuzarea volumului enorm de date în timp real pe tot globul. Operaţiile informaţionale includ sisteme de informare care obţin, produc, prelucrează şi difuzează informaţii. O structură dinamică a INFOSYS este esenţială pentru comandanţi în scopul cunoaşterii situaţiei şi al vizualizării câmpului de luptă. Aceste sisteme de informare afectează modul în care se desfăşoară conducerea luptei. Viziunea asupra câmpului de luptă este întărită prin informatizare. Caracteristicile obiectivelor proprii şi ale inamicului pot fi localizate şi afişate pe display pentru comandanţi, asigurându-le acestora actualizarea datelor situaţiei curente. S-au dezvoltat sisteme de sesizoare pentru

tragere care utilizează unde infraroşii sau milimetrice pentru a vedea şi a auzi cu sesizoare acustice, a simţi energia seismică, a interpreta informaţiile culese, a decide dacă acestea percep o ţintă pe baza unor criterii prestabilite şi a angaja folosirea unor calculatoarc miniaturale de mare viteză.

Cunoaşterea situaţiei de pe câmpul de luptă este dezvoltată într-o măsură fără precedent. Prin sisteme de informare moderne şi prin operaţii informaţionale, comandanţii vor fi capabili să gestioneze mai bine caracterul de incertitudine al războiului. În viitoarele operaţii terestre întrunite, coerenţa forţei (şi, astfel, aplicarea capacităţii de luptă) poate fi realizată mai degrabă printr-o bună cunoaştere a condiţiilor de pe câmpul de luptă decât prin măsuri fizice de control tradiţionale, cum ar fi măsurile grafice de control sau demarcarea geografică a zonelor de operaţii. Sistemele de informare viitoare vor avea atât componente militare secrete de sine stătătoare, cât şi componente civile nesecrete. Securitatea acestor sisteme prezintă o importanţă absolută pentru succesul operaţiilor informaţionale. Operaţia informaţională are la bază faptul că persoana potrivită primeşte informaţia potrivită în locul potrivit.

3.3. Cercetarea, obţinerea de date, culegerea de informaţii (RII).

Datorită dezvoltării tehnologice, trăim într-o lume a informaţiilor. Un aspect critic al operaţiilor informaţionale este realizarea RII astfel încât să-i facă capabili pe comandanţi să-şi focalizeze eforturile. Aceasta este cheia pentru realizarea cunoaşterii situaţiei. Unul din obiectivele Forţei XXI este de a folosi informaţiile obţinute pentru a realiza o viziune comună a câmpului de luptă la toate nivelurile şi în timp real. Obţinerea acestor informaţii nu este numai responsabilitatea organelor de cercetare. Pentru realizarea unui înalt nivel de fidelitate, comandanţii trebuie să folosească toate mijioacele şi sursele disponibile.

Cheia desfăşurării operaţiilor informaţionale este pregătirea informativă exactă şi la timp a câmpului de luptă (IPB).Conturarea operaţiei informaţională trebuie să depăşească sfera tridimensională a câmpului de luptă şi să cuprindă informaţii despre capacităţile, disponibilităţile şi vulnerabilităţile tehnologiei. În plus, într-o lume interconectată, trebuie avut în vedere impactul pe care acţiunile noastre îl pot avea asupra sistemelor proprii şi ale inamicului. Necesităţile de informare critice ale unui comandant pentru operaţia informaţională le depăsesc mult pe cele din trecut. Informarea trebuie să răspundă la următoarele întrebări:

1 – Cum funcţionează sistemele de informare ale inamicului şi care sunt vulnerabilităţile sale?

2 – Cum acţionează ciclul de decizie al inamicului?

3 – Care sunt punctele sale nodale?

4 – Care sunt sursele sale de autoritate şi de legitimitate?

5 – Cum funcţionează societatea sa?

6 – Ce capacităţi de atacare a sistemelor aliaţilor are?

În măsura în care se schimbă necesităţile, trebuie să se schimbe şi personalul de informaţii. Acesta trebuie să prelucreze acum informaţii din surse netradiţionale, ca INTERNET şi alte medii globale de informare. Coordonarea celor trei componente ale operaţiei informaţionale va genera un efort integrat pe deplin care ne va da posibilitatea să obţinem dominantă informaţională şi avantaj operativ. Acestea sunt concepte integrate şi căi sporite de abordare a conflictelor şi a luptei în era informaţiilor.

3.4. Potenţialul operaţiei informaţionale

Operaţia informaţională este desfăşurată permanent pentru a descuraja agresiunea, pentru a-i asigura pe aliaţi sau pentru a constrânge inamicul, toate acestea în sprijinul intereselor naţiunii proprii. Dacă este desfăşurată destul de timpuriu şi cu succes, operaţia informaţională poate preveni conflictele, reduce pierderile sau stabiliza rapid

condiţiile. Pentru comandanţi, operaţia informaţională este un multiplicator de luptă. A şti unde, când şi cum să dai lovitura decisivă inamicului, interzicându-i acestuia aceeaşi capacitate, reprezintă un avantaj fenomenal. Prin operaţia informaţională se pot concentra rapid şi eficient efectele.

În alte operaţii decât cele de război se poate aplica operaţia informaţională pentru controlul situaţiei. În operaţia JOINT ENDEAVOR din Bosnia, operaţia informaţională a fost desfăşurată 24 de ore din 24. Prin operaţia informaţională, IFOR cunoştea întotdeauna unde se aflau şi ce făceau facţiunile rivale. Acest lucru a făcut ca IFOR să poată controla situaţia în termenii săi. Interacţiunea constantă cu mass-media şi mesajul de speranţa trimis populaţiei prin operaţiile psihologice şi afacerile civile au constituit elementele principale ale succesului în Bosnia. Acţiuni Ic operaţiei informaţionale desfăşurată de IFOR au prevenit conflictele din acea regiune.

Obiectivele operaţiei informaţionale scot în evidenţă, de asemenea, noi modalităţi de gândire despre atacarea sau apărarea centrelor de gravitaţie. Folosind capacităţile neletale ale operaţiei informaţionale, se poate ataca un centru de gravitaţie pentru subminarea legitimităţii sau acţiunilor inamicului. Rezultatul final poate fi atât prevenirea escaladării conflictului, cât ci contribuţia la o victorie decisivă.

Pe măsură ce guvernul, societatea şi armata unei ţări devin inexorabil legate prin dependenţa lor de diferitele infrastructuri de informare, apar noi vulnerabilităţi. Accentul operaţiei informaţionale se pune pe analiza nodală a vulnerabilităţilor principale proprii şi ale inamicului. Operaţia informaţională poate viza conducerea, procesul de luare a hotărârilor şi C2 ale inamicului, poate crea potenţialul de a controla sistemul procesului decizional al adversarului şi cauza chiar colapsul acestuia. Capacităţile de atac derivate din operaţia informaţională şi puterea cipurilor de calculator asigură posibilităţi de

succes mai mari decât cele rezultate din folosirea armamentului cu energie cinetică.

În acelaşi timp, aspectele defensive ale operaţiei informaţionale sunt la fel de importante pentru protejarea propriilor vulnerabilităţi şi centre de gravitaţie.

Măsurile ŒW, ca operaţiile psihologice, lupta electronică şi distrugerea, constituie factorii-cheie în executarea unei campanii de operaţii informaţionale. Folosirea lor combinată, împreună cu capacităţi modeme de culegere a datelor, de supraveghere şi de cercetare, îi asigură comandantului instrumente pentru o campanie managerială bazată pe o percepţie reală, astfel încât poate încerca să influenţeze emoţiile, motivele şi raţionamentul obiectiv al inamicului. Dacă reuşeşte, campania operaţiilor informaţionale poate afecta conducerea inamicului sau sprijinul populaţiei în aşa măsură încât să anticipeze conflictul şi să permită realizarea scopurilor fără a pune soldaţii americani în pericol.

Totuşi, când lupta este inevitabilă, o operaţie informaţională reuşită va reduce în mare măsură pierderile pentru că vom avea mai multe informaţii decât inamicul şi vom putea controla ritmul conflictului. Aceşti factori sporesc viabilitatea şi importanţa operaţiei informaţionale în apărarea şi promovarea intereselor SUA în lume.

Astăzi, comandamentele regionale dezvoltă variate opţiuni flexibile de descurajare (FDO) pentru a reduce tensiunea şi a descuraja agresiunea înainte de izbucnirea ostilităţilor. Aceste metode includ sancţiunile economice, blocadele sau demonstraţiile militare de forţă. Cu ajutorul operaţiei informaţionale comandanţii pot dezvolta opţiuni flexibile de descurajare extinse dincolo de aceste metode mai tradiţionale. Dată fiind proliferarea mediului global informaţional, tehnicile operaţiei informaţionale pot deveni „opţiunea flexibilă de descurajare de prima mână” într-o criză. Exploatarea vulnerabilităţilor infrastructurii inamicului şi afectarea procesului de luare a hotărârilor de către acesta se numără printre posibilele opţiuni flexibile de descurajare care ar ajuta la rezolvarea unei crize

înaintea transformării acesteia în conflict armat. Astfel de acţiuni reclamă o coordonare strânsă şi, cel mai probabil, o aprobare interagenţii. În acest mod operaţia informaţională va deveni o componentă integrală a capacităţilor noastre de proiecţie a puterii.

Activităţile strâns coordonate şi sincronizate ale afacerilor publice au devenit vitale în acest mediu. Afacerile publice corecte şi oportune – în care comandanţii sunt văzuţi făcând tot ceea ce depinde de ei pentru a prezenta adevărul – sunt importante pentru desfăşurarea operaţiei informaţionale şi vor ajuta la descurajarea agresiunii, la liniştirea şi sprijinirea aliaţilor şi la obligarea celor cu care ne luptăm să ne accepte voinţa.

Definirea modului nostru de a lupta va depinde, în parte, de noi reguli de angajare în luptă. Acestea constituie o provocare însemnată pentru operaţia informaţională.

Datorită caracterului articulat al mediului global de informare şi folosirii în comun a platformelor de informare trebuie să se analizeze cu atenţie modul în care să fie vizat sistemul de informare al inamicului, deoarece ceea ce se face ar putea avea impact asupra unor *terţi neutri*. *O* altă situaţie grea ar putea avea loc dacă s-ar hotărî neutralizarea unei reţele electrice care alimentează spitalele inamicului sau sistemele de control al traficului. Natura atotcuprinzătoare a INFOSYS va continua să influenţeze dezvoltarea, limpezirea şi dezbaterea regulilor de angajare a operaţiilor informaţionale atât în timp de pace, cât şi de Război.

3.5. Organizarea desfăşurării operaţiilor informaţionale ale trupelor de uscat

Pentru a concentra eforturile trupelor de uscat spre acest aspect important al luptei, gl. Reimer a declarat, în septembrie 1996, ca intenţia lui este de a instituţionaliza operaţiile informaţionale, care sunt vitale pentru modul în care trupele de uscat desfăşoară operaţiile. Pentru aplicarea în practică a acestei intenţii, o serie de organisme răspund de integrarea operaţiilor informaţionale în trupele de uscat.

3.6. Triada pentru operaţiile informaţionale ale Statului Major al Departamentului Trupelor de Uscat (HQDA).

S-a stabilit o triadă constând din oficiile adjunctului şefului statului major pentru operaţii şi planuri (DCSOPS), adjunctului şefului statului major pentru informaţii (DCSINT) şi directorului sistemelor de informare pentru comandă, control, transmisiuni şi calculatoare (DISC4). Triada primeşte directive de la secretarul Departamentului Trupelor de Uscat şi de la şeful Statului Major al Trupelor de Uscat şi asigură unitatea eforturilor celor trei componente ale operaţiilor informaţionale. În cadrul triadei, punctul central este DCSOPS.

3.7. Comandamentul pentru Instruire şi Doctrină al Trupelor de Uscat (TRADOC).

Comandantul Centrului Armelor întrunite de la Fort Leavenworth, Kansas, este cel care propune operaţiile informaţionale ale TRADOC. Centrul răspunde de dezvoltarea doctrinei operaţiilor informaţionale (FM 100-6), de instruire, de dezvoltarea conducerii, de problemele de organizare, materiale şi de Personal. Acum, după ce regulamentul FM 100-6 a intrat în vigoare, următoarea lui sarcină este de a dezvolta tactica, tehnica şi procedeele (TTP) operaţiilor informaţionale. Viitorul manual pe această temă va prezenta modul de planificare şi executare a operaţiilor informaţionale la nivel corp de armată şi divizie. De asemenea, el este pe cale de a incorpora operaţiile informaţionale în programa şi exerciţiile diferitelor şcoli, inclusiv în Programul de pregătire a conducerii luptei (BCTP) pentru corpuri de armată şi divizii şi în exerciţiul PRAIRIE WARRIOR pentru cursanţii Colegiului de Comandă şi Stat Major.

3.8. Activitatea de luptă informativă terestră (LIWA). Situat la Fort Belvoir, Virginia, LIWA este un organism important pentru implementarea operaţiilor informaţionale în trupele de uscat. Acesta repartizează echipele de sprijin în campanie (FST) pentru întărirea statelor majore de campanie ale comandanţilor şi asigură experienţa tehnică

în materie de operaţii informaţionale pe carc statele majore nu o au. Echipele coordonează, planifică şi sincronizează diferitele elemente ale operaţiilor informaţionale pentru a facilita executarea acestora în timpul operaţiilor militare. Echipele de sprijin în campanie îi consiliază pe comandanţi în privinţa operaţiilor importante de atacare a comenzii şi controlului inamicului şi celor de protejare a comenzii şi controlului propriu. O astfel de echipă a asistat trupele de uscat din Europa în elaborarea planului de protejare a comenzii şi controlului pentru operaţia JOINT ENDEAVOR şi a continuat să sprijine IF OR. Echipele LIWA acţionează, de asemenea, împreună cu statele majore din componenţa trupelor de uscat în timpul exerciţiilor importante şi situaţiilor de urgenţă reale din lume.

Cea mai nouă misiune a LIWA este înfiinţarea unei echipe de reacţie la problemele intervenite în reţelele de calculatoare ale trupelor de uscat (ACERT). Această echipă are capacitatea de a răspunde la situaţiile de penetrare sau atacare a reţelelor protejate sau neprotejate. În cazul unor astfel de incidente, echipa va identifica problema, va institui controlul, va repara daunele aduse sistemului şi va coordona măsurile contrainformative sau de sprijinire a întăririi legislaţiei.

3.9. Necesităţile de pregătire în vederea operaţiilor informaţionale.

Dezvoltarea calităţilor necesare conducătorilor şi militarilor pentru desfăşurarea viitoarelor operaţii informaţionale va necesita timp şi resurse. În prezent, trupele de uscat au militari pregătiţi pentru activităţi ale operaţiei informaţionale ca afacerile civile, operaţiile psihologice şi lupta electronică, dar puţini sunt cei care dispun de o bază sau de antrenament în ceea ce priveşte totalitatea conceptelor operaţiei informaţionale.

Oricine poate începe să devină competent în unele aspecte ale IQ, cum ar fi protejarea C2. Managerii şi utilizatorii sistemului au nevoie de pregătire nemijlocită privind bazele securităţii sistemului şi reţelei. Trupele de

uscat pregătesc cursurile necesare. Totuşi, această instruire poate fi realizată printr-o varietate de alte surse. Chiar fără o pregătire formală, utilizatorii calculatoarelor – orice militar din forţa informatizată a trupelor de uscat – pot ajuta la câştigarea războiului informaţional. Lucruri simple ca protejarea parolelor, verificarea antivirus a dischetelor înainte de copierea fişierelor de pe acestea şi supravegherea calculatoarelor pornite vor întări în mare măsură siguranţa lucrului. Operaţiile informaţionale trebuie integrate în exerciţiile de nivel unitate şi în programa centrelor de instrucţie de luptă.

3.10. Responsabilităţi ale conducerii operaţiilor informaţionale.

Comandanţii pot să înceapă încorporarea operaţiilor informaţionale prin a cere statelor majore să se familiarizeze cu prevederile regulamentului FM 100-6. De asemenea, ei trebuie să pună două întrebări, şi anume:

are nevoie corpul de armată, divizia sau gruparea operativă – tactică de o celulă ad-hoc pentru operaţii informaţionale?

cum va integra eşalonul respectiv operaţiile informaţionale în planurile de urgenţă sau în exerciţii?

3.11. Celula pentru operaţii informaţionale – o variantă a unei astfel de celule ar trebui să cuprindă un ofiţer cu IO/C2W Asemenea funcţie sau specialitate nu există în prezent, dar este necesară. Ofiţerul respectiv va trebui nu numai să aibă cunoştinţa de bază privind toate aspectele IO şi C2W, şi mai important, să fie capabil să sincronizeze operaţia informaţională pentru a sprijini planul şi intenţia generală a comandantului. De asemenea, va trebui să se ceară o echipă de sprijin în campanie de la LIWA pentru a ajuta la planificarea şi coordonarea operaţiei informaţionale.

4. OPERAŢIILE INFORMAŢIONALE PENTRU SITUAŢIILE DE URGENŢĂ

Deoarece operaţia informaţională este aplicabilă atât în timp de pace cât şi de război, următoarele exemple arată modul în care comandanţii ar putea integra IO în

planurile şi operaţiile pentru situaţii neprevăzute. Aceste exemple sunt principiale, dar dificultatea pentru comandanţi constă în orchestrarea şi armonizarea multitudinii de componente ale operaţiei informaţionale.

4.1. Dislocarea unui corp de armată în Orientul Mijiociu – misiune de impunere: Împreună cu alte forţe întrunite şi de coaliţie din zonă, se întocmeşte un plan detaliat al C2W pentru izolarea şi subminarea conducerii inamicului; coordonarea interagenţii, cu valorificarea mijioacelor naţionale, este desfăşurată pentru asigurarea unui plan integrat; analiza nodală a infrastructurilor inamicului este completată cu aceea a profilului personalităţilor din conducerea inamicului; o campanie de gestionare a percepţiei este prestată pentru a rupe orice coaliţie pe care inamicul ar putea să o realizeze cu statele vecine; această campanie vizează şi sprijinul populaţiei pentru guvernul inamicului; în acelaşi timp, se desfăşoară o puternică operaţie de a face publice pentru întărirea sprijinului intern faţă de acţiunile noastre; se fac evaluări de vulnerabilitate pentru identificarea deficienţelor sistemelor proprii astfel încât să putem proteja comanda şi controlul; se iau măsuri de securitate întărită a infrastructurii forţelor armate de pe continentul american şi a celor ce îşi au baza pe alte continente; toate acţiunile sunt sincronizate pentru a permite pătrunderea rapidă şi fără opoziţie în regiune, pentru stabilizarea zonei şi reducerea riscurilor la adresa militarilor americani.

4.2. Desfăşurarea unei divizii în Europa de Est – misiune de întărire a păcii: În cadrul unei misiuni a NATO, divizia îşi organizează o celulă IO în cadrul biroului G3 (operaţii); această celulă îşi centrează eforturile în direcţia asigurării sprijinului informativ pentru legitimarea generală a implicării SUA în misiune şi pentru realizarea stabilităţii în regiune; celulă IO primeşte date de la o varietate de elemente, printre care forţele speciale, contrainformaţiile şi alte mijioace de culegere a datelor din zonă, apoi foloseşte toate informaţiile pentru a coordona acţiunile de afaceri publice şi civile în zona de operaţii. În

plus, personalul celulei asigură ca temele operaţiilor psihologice şi „mesajul” elaborat pentru operaţie să fie integrate în planurile sale. Mesajul operaţiilor psihologice trebuie să fie elastic şi energic pentru a promova o pace mai durabilă şi stabilizarea regională. Comandantul diviziei stabileşte necesităţile de informaţii critice privind fracţiunile aflate în luptă şi protecţia forţei proprii; celula IO elaborează un plan de protejare a C2 bazat pe o analiză a riscurilor la adresa diferitelor sisteme şi reţele; pentru asigurarea succesului misiunii de întărire a păcii, celula IO trebuie să aibă permanent în vedere realizarea legitimării implicării forţelor americane.

4.3. Desfăşurarea unei brigăzi în Africa – misiune de asistenţă umanitară: o grupare operativă la nivel brigadă, aflată sub egida ONU, se desfăşoară pentru a ajuta la realizarea operaţiilor de ajutorare şi pentru protejarea liniilor de aprovizionare a refugiaţilor; obiectivul operaţiei de informare este nu numai de a sprijini acţiunile de ajutorare, ci şi de a demonstra rolul pozitiv pe care îl au forţele americane în cadrul operaţiei; comandantul grupării operative cere de la LIWA o echipă de sprijin în campanie pentru a ajuta la coordonarea planului IO; această echipă cooperează cu organele de informaţii pentru identificarea specificului culturii şi populaţiei locale, lucru care va ajuta la elaborarea unui plan IO viabil; esenţială pentru succesul misiunii este coordonarea strânsă cu organizaţiile neguvernamentale, cu partenerii de coaliţie şi cu fracţiunile combatante; planificatorii operaţiei trebuie să aibă în vedere integrarea acestor grupuri în celula IO, este foarte importantă stabilirea modului de realizare a legăturii cu ele într-o zonă în care mijloacele de comunicaţii interne sunt puţine sau lipsesc cu desăvârşire; comandantul analizează cea mai bună modalitate de obţinere a informaţiilor pentru salvarea vieţii refugiaţilor şi urmăreşte să se realizeze activităţi de afaceri publice şi civile solide.

Exemplele evidenţiază doar parţial complexitatea operaţiilor informaţionale. Acestea reclamă analize intense

şi detaliate, planificare şi coordonare. Totuşi, exemplele scot în evidenţă unele consideraţii pe care comandanţii trebuie să le evalueze pentru a optimiza capacităţile şi misiunile operaţiilor informaţionale.

4.4. Implicaţiile operaţiilor informaţionale

Operaţia informaţională nu constituie un fel de „glonţ de argint" pentru obţinerea victoriei în viitoarele conflicte dar, aşa cum sublinia preşedintele Comitetului întrunit al Statelor Majore, gl. John Shalikashvili: *„Proliferarea explozivă a tehnologiilor din domeniul informaţional are un impact semnificativ asupra luptei în toate fazele sale, asupra întregii game de operaţii militare şi asupra tuturor nivelurilor* războiuluiAstfel, importanţa operaţiilor informaţionale nu trebuie exagerată. Ele constituie pentru comandanţi un mijioc de asigurare a unui nivel de cunoaştere şi de înţelegere a conducerii luptei niciodată atins până în prezent.

Într-o lume interconectată, bazată pe şi pusă în mişcare de INFOSYS, necesitatea protejării infrastructurii şi a cetăţenilor noştri va constitui o provocare deosebită. Totuşi, aceasta este o lume care poate fi exploatată în interesul nostru.

5. RĂZBOIUL MEDIATTC

Comunicarea de tip mediatic este expresia relevantă a democraţiei unui sistem politic, iar relaţia dintre ele este atât de strânsă şi direct proporţională încât niciuna nu poate fi concepută fără cealaltă. Astfel, cu cât structurile comunicării sunt mai cuprinzătoare şi mai accesibile, cu atât există mai multe şanse potenţiale de afirmare a democraţiei.

Expansiunea comunicării în general şi mai cu seamă a celei de masă este determinată de cerinţele informative şi cognitive toi mai sporite ale individului, precum şi de nevoia societăţii de autoreglare. Aceşti factori determinanţi îşi subordonează instantaneu tehnologiile de vârf încât au reuşit să plaseze fenomenul comunicării de masă în prim-planul vieţii cotidiene, capacitatea tehnicilor multimedia de transmitere şi redistribuire a informaţiilor

lărgind extraordinar atât sfera publicului, cât, mai ales, pe acea a resurselor de informare, documentare şi divertisment. Altfel spus, implementarea *high-tech* în comunicare i-a conferit acesteia eficienţa deplină, socializând-o de o manieră atât de masivă încât sintagma lui Marschall Me Luhan despre „satul global" aproape că nu mai exprima o realitate, ci o banalitate.

Nu numai că rapiditatea, diversitatea şi volumul informaţiei trebuie asociate cu libera circulaţie a informaţiei, cu egalitatea accesului la informare şi, nu în ultimul rând cu garantarea informării corecte a cetăţeanului. Acestea, deşi sunt principii înscrise în Declaraţia Universală a Drepturilor Omului, continuă a rămâne deziderate de împlinit pentru o viitoare ordine mondială, deoarece, ca şi democraţia, libertatea informaţiei este acum, fără îndoială, inegal răspândită în lume. Mai mult chiar, ea rămâne tributară societăţii în care se manifesta, fapt subliniat, printre mulţi alţii, de profesorul Hervé Bourges: «Libera circulaţie prezintă toate defectele liberalismului economie. Aceasta înseamnă că ea se face în folosul celor mai puternici şi în detrimentul celor slabi. *Laissez/ dire*, *laissez paser* este legea junglei, în afara cazului când toţi ar avea aceleaşi şanse şi mijioace. Or, este limpede că şansele şi mijioacele ţărilor *lumii a treia*, în sfera informaţiei sunt mult inferioare şi că decalajele, ca şi în celelalte domenii, continuă să se adâncească".

Prin urmare, dezechilibrul manifestat în propagarea informaţiei nu are numai explicaţii istorice şi tehnologice, ci este reflexul interesului şi propagandei de sorginte economică, financiară şi politică, manipulate cu abilitate de trusturile transnaţionale de presă şi nu numai. Acest dezechilibru este cultivat zi de zi de marile puteri politico-economice ale lumii în dauna ţărilor mici şi mijlocii, pe coordonate biunivoce când se produce pe axa estvest. Şi univoce, întotdeauna dinspre nord înspre sud. Fapt ce se realizează aproape fără băgare de seamă, întrucât informaţia cu sens unic se insinuează perfid în conştiinţele

oamenilor, afectându-le cadrul de viaţă în cele mai diverse moduri, dar mai totdeauna cu efecte scontate.

În general, informaţia, fie ea politică, economică, culturală etc., este expresia interpretant coerente a realităţii complexe dintr-o anumită unitate de timp şi dintr-un anumit loc. Ea concentrează un punct de vedere asupra lumii. Într-o oarecare măsură, valoarea informaţiei este în strânsă legătură cu difuzarea ei. La baza acestei operaţii stă un proces complex de selecţie şi ierarhizare întemeiată pe criterii ideologice precise. Din puzderia de fapte şi evenimente care dau substanţă unei zile la scară planetară, marile agenţii de presă, marile companii de radio şi televiziune aleg 100-200 pe care le ierarhizează într-un anumit mod şi apoi le difuzează. Desigur, este greu să pretinzi obiectivitate absolută în acest proces delicat şi, în acelaşi timp, dificil, dar este inacceptabil ca el să fie transformat într-o metodă deosebit de subtilă de falsificare a realităţii, în conformitate cu interesele şi ideologia promovate de ziarişti şi mijloacele de comunicare ce se erijează în principalele surse de informare „obiectivă” şi „corectă” a lumii. Am folosit ghilimelele pentru obiectivă şi corecte căci aşa cum cineva a observat deja, în momentul de faţă aproape că nu mai există informaţie neutră ci numai „informaţie de luptă”, adică avem de-a face cu transformarea tezei în informaţie prin deghizarea funcţiilor militante în funcţii informative.

Odată ajunşi aici se impune constatarea existenţei unor centre de putere informaţională interesate să dea „ştirii”, „comentariului” şi imaginii direcţia şi conţinutul conforme unor intenţii şi scopuri manifestate. Procedeul presupune utilizarea cu bună ştiinţă a unui arsenal de mijioace şi tehnici de falsificare şi manipulare a informaţiei, care verificate şi identificate de specialişti le pot furniza acestora argumente că se află în plin război mediatic, componenţa esenţială a războiului psihologic. În principiul ei, au în vedere cinci posibilităţi strategice:

1. se acordă proeminenţă unor fapte fără importanţă reală, nerelevante, în detrimentul celor cu adevărat

importante, sau se amestecă nedistinct ştirile nesemnificative cu cele semnificative.

2. difuzarea unor ştiri fragmentare în locul celor complete, sau asamblarea unor informaţii parţiale, pentru a crea impresia unui adevăr complet.

3. prezentarea ştirilor într-o manieră care să conducă la interpretări şi concluzii eronate, favorabile intereselor particulare.

4. Înfăţişarea evenimentelor într-un mod de natură să provoace îndoieli şi temeri nejustificate sau chiar exagerate, cu intenţia de a influenţa sau condiţiona acţiunile ulterioare ale indivizilor, comunităţilor de orice tip, naţiunilor sau guvernelor.

5. trecerea sub tăcere a faptelor, evenimentelor care se presupune că ar suscita anume reacţii din partea publicului sau a altui destinatar, combinate, eventual cu supralicitarea altora, în dorinţa de a le estompa pe cele dintâi.

Este, dacă vreţi, partea văzută a icebergului!

Partea ne văzută, covârşitoare este destinată superprofesioniştilor informaţiei. Este câmpul de bătălie pe care se înfruntă şi se desfăşoară forţe atât de copleşitoare încât doar un război convenţional poate fi invocat ca termen de comparaţie, dar şi în acest caz numai pentru estimarea cheltuielilor materiale şi mai puţin a rezultatelor politico-economice, de multe ori mult mai eficiente în cazul războiului informaţional. Efectul său este devastator demoralizarea şi inducerea ideii în mediile elitei jurnalistice mondiale că informarea corectă a devenit imposibil de depistat – şi cu atât mai puţin de utilizat şi propagat – este cea dintâi şi cea mai importantă bătălie câştigată de războiul mediatic. Este o victorie psihologică! Adică esenţialul în orice tip de război! Restul... restul ţine de tehnică, de tactică şi strategie, de arta de a dirija pionii informaţionali pe tabla de şah a acestui război ce se va sfârşi doar o dată cu civilizaţia care i-a dat naştere şi-l întreţine zi de zi, ceas de ceas, minut de minut.

„Cea dintâi dintre forţele care conduce lumea este

minciuna”; afirmă Jean-François Revel, unul dintre marii ziarişti ai timpului nostru în deschiderea volumului *Cunoaştere inutilă*, volum prin care doreşte să demonstreze că într-o lume copleşită de minciună mediatizată, – cum brutal numeşte el dezinformarea –, a vrea sau a mai putea să înţelegi ceva din ce se întâmplă pe mapamond a devenit o întreprindere „inutilă”, sortită de la bun început eşecului. Căci, proclama la rându-i Simone Weil: „Epoca noastră este atât de otrăvită de minciună încât transformă în minciună tot ce atinge. Şi noi suntem ai epocii: nu avem niciun motiv să ne vedem mai buni decât ea”.

Or, cum minciuna de dragul minciunii nu există, deoarece minciuna înseamnă „denaturarea intenţionată a adevărului având de obicei ca scop înşelarea cuiva”, rămâne de fiecare dată a şti să identifici sursa minciunii, interesul care a determinat „punerea ei la lucru” şi, nu în ultimul rând „ţinta şi efectele scontate. Profesional vorbind, a identifica sursele şi cauza dezinformării şi a-i neutraliza efectele.

Întrucât în războiul mediatic dezinformarea deţine locul strategie central, toate celelalte mijioace utilizate – precum intoxicarea, provocarea, propaganda, publicitatea dirijată – nefiind decât atributele sale factice, găsim esenţială definirea sa cât mai exactă.

Se recurge la dezinformare deoarece se crede în puterea cuvântului şi, în ultimul timp din ce în ce mai mult, a imaginii de a „disloca” inamicul. Spre deosebire de dezinformarea folosită în timp de război – preponderent militară – şi de intoxicarea reciprocă a serviciilor secrete, în general permise şi încadrate în sfera vicleniilor de luptă admise, dezinformarea pe timp de pace – cu precădere mediatică – are ca scop voinţa permanentă de „distrugere a întregului sistem de cunoaştere obiectivă a realităţii într-o societate data”, cum remarca în 1984 C. Meinik.

Că dezinformarea a devenit o realitate cotidiană abia în timpul nostru ne-o dovedeşte faptul că până nu de mult dicţionarele – inclusiv cele româneşti – nu cunoşteau decât

accepţiunea comună reieşită prin alăturarea logică a vocabularelor *dcz+informa*, adică „a informa (cu bună ştiinţă) în mod greşit”. Termenul purtător al unei conotaţii speciale a fost introdus pentru prima dată după cel de-al doilea război mondial în Marea Enciclopedie Sovietică – firește îmbibat de ideologia comunistă – iar în Dicţionarul Academiei Franceze abia în 1984, unde are următoarea definiţie: „Acţiune intermitentă sau continuă – prin folosirea oricărui mijioc – ce constă în inducerea în eroare a unui adversar sau în favorizarea subversiunii în rândurile acestuia în scopul de a-l slăbi”.

Chiar şi aşa explicaţia rămâne nesatisfacătoare, obligându-ne să apelăm la specialiştii în domeniu care cunosc dezinformarea în mod nemijiocit. Astfel, însuşi părintele K.G.B.-uhii, Dzerjinski, fixând misiunile şi metodele C.E.K. A. stabilea încă din 1917 un sistem de ofensivă mediatică, destinat compensant forţelor armate sovietice: „Comuniştii trebuie să fie pregătiţi să folosească la nevoie tot felul de şiretlicuri, planuri şi stratageme ilegale, să nege şi să ascundă adevărul. Politica comunistă vizează în mod concret învrăjbirea în rândurile inamicilor [...]. Cuvintele mele erau alese în aşa fel încât să provoace ura şi confuzia, nu pentru a convinge adversarul, şi pentru a-l disloca; nu pentru a-i îndrepta greşelile, ci pentru a-l distruge măturându-i structurile de pe suprafaţa globului”, (după John Barron, *K.G.B.*, Paris, 1975)

G. Veraldi, în prefaţa lucrării lui Pierre Nord, *L ' Intoxication*, apărută la Paris în anul 1971, indică scopul dezinformării pe cât de concis, pe atât de lămuritor:

„Crearea unei realităţi false atât de convingătoare încât adversarul să o creadă justă”.

Iar celebrul sovietolog Alexandr Zinoviev reuşeşte, în *Para Bellum*, să exprime superlativul în materie:

„Inamicul trebuie să acţioneze aşa cum dorim noi, spre folosul nostru, dar fiind convins că acţionează conform propriei voinţe, deci împotriva intereselor noastre”.

Însă cea mai explicită şi profesională definiţie am

aflat-o în volumul *Le temps de la desinformation* (Paris, 1986) de Henri- Pierre Cathala, apărut în traducere românească în 1991 cu titlul *Epoca dezinformării*, volum de autoritate în materie, care ne-a fost de un real folos în elaborarea prezentei comunicări şi pe care îl recomandăm cu căldură tuturor specialiştilor ca pe un manual fundamental:

„Dezinformarea reprezintă ansamblul procedeelor dialectice puse în mod intenţionat pentru a reuşi <manipularea > perfectă a persoanelor, grupurilor sau a unei întregi societăţi, în scopul de a le devia conduitele politice, de a le domina gândirea sau chiar de a le subjuga. Presupune disimularea surselor şi scopurilor reale, precum şi intenţia de a face rău, printr-o reprezentare deformată sau printr-o interpretare tendenţioasă a realităţii. Se înscrie în rândul acţiunilor psihologice subversive".

Plecând de la această definiţie – cum, de altfel, este lesne de intuit – războiul mediatic presupune nu numai existenţa unor instituţii şi cadre specializate, dar mai ales alocarea de mijloace logistice excepţionale, întotdeauna direct proporţionale cu voinţa şi gradul de implicare pe mapamond a forţei politice sau economice respective. Pentru a ne face o imagine cât de cât lămuritoare asupra realităţii vom recurge la un pasaj mai detaliat din cartea lui Thiery Wolton, *K.G.B.-ulân Franţa* (Paris 1986; Bucureşti, 1992) referitor la ce înseamnă acest război pentru fosta U.R.S.S., cu convingerea că dacă amănuntele rămân valabile pentru timpul şi locul la care se face referire precisă, esenţa aspectului poate fi avută în vedere, *mutatis mutandis*, pentru înţelegerea de principiu a unor realităţi similare:

„Patruzeci de miliarde de franci este cifra anuală de afaceri a unei întreprinderi ca *Michelin* sau o dată şi jumătate suma de care dispune în fiecare an Ministerul Francez al Afacerilor Externe pentru a-şi asigura funcţionarea şi a promova imaginea Franţei în lume.

Patruzeci de miliarde este şi suma pe care U.R.S.S. O cheltuieşte anual pentru măsuri active şi dezinformare,

vârf de lance al războiului ideologie pe care-l duce împotriva ţărilor democratice, pentru a le destabiliza.

Sintagma măsuri active a apărut în vocabularul sovietic în cursul anilor 1950 pentru a desemna un anumit număr de mijloace oficiale şi clandestine puse în operă pentru a acţiona asupra cursului evenimentelor, comportărilor şi opţiunilor politice ale ţărilor străine. Prin intermediul lor, U.R.S.S. Încearcă să facă presiuni asupra deciziilor guvernamentale ale altor state, să submineze încrederea populaţiei în conducătorii ei şi în instituţii, să suscite tensiuni în relaţiile internaţionale, să-şi discrediteze adversarii sau, în orice caz, să le slăbească poziţiile. *Măsurile active* prezintă în general o viziune deformată a realităţii pentru a înşela ţinta, fie un guvern străin, fie cercurile politice sau opinia publică a unei ţări.

Există două feluri de măsuri active. Deschise, atunci când acestea se aplică propagandei oficiale şi relaţiilor diplomatice normale: secrete, atunci când este vorba de propaganda clandestină, despre dezinformarea scrisă sau orală, despre activitatea agenţilor de influenţă şi, în fine, despre organizaţiile de masă subminate de sovietici.

În anii '80, măsurile active au devenit o prioritate pentru subversiunea sovietică, ca şi spionajul ştiinţific şi jefuirea tehnologiilor occidentale. Lupta împotriva dezinformării este deci esenţială astăzi pentru însăşi supravieţuirea democraţiilor. Dar în societăţile noastre deschise şi libere este adeseori foarte greu ca ea să fie combătută. Libera circulaţie a informaţiei şi dreptul oricui de a gândi, de a vorbi şi de a scrie sunt sistematic utilizate de către U.R.S.S. pentru tulburarea opiniei publice şi dezechilibrarea guvernelor occidentale.

Este adeseori dificil de făcut distincţie între dezinformarea propriu-zisă şi exprimarea opiniilor. Uniunea sovietică ştie să se adăpostească în spatele acestei distincţii pentru a-şi difuza clandestin propaganda sau pentru a intoxica opinia publică prin intermediul agenţilor de influenţă complici (plătiţi) sau pur şi simplu manipulaţi (pe care Lenin îi numea deja *idioţii necesari*)

[...]. La Moscova, cel puţin două mii de persoane se ocupă numai cu măsurile active. Pentru a concepe, a planifica, a difuza dezinformarea, U.R.S.S. dispune de o organizaţie complexă, de o întreagă reţea în care fiecare fir este legat la cel mai înalt nivel, de Biroul Politic al partidului [...]. Secţia Internaţională administrează, coordonează şi finanţează zeci de organizaţii de masă însărcinate cu manipularea opiniei publice mondiale, popularizând campaniile de propagandă elaborate de Moscova pentru susţinerea obiectivelor sale politice: Consiliul Mondial al Păcii, Federaţia Sindicală Mondială, Organizaţia de

Solidaritate cu Popoarele din Africa şi Asia, Federaţia Mondială a Tineretului Democratic, Uniunea Internaţională a Studenţilor, Organizaţia Internaţională a Ziariştilor, Conferinţa Creştină pentru Pace, Federaţia Internaţională a Femeilor Democrate, Asociaţia Internaţională a Juriştilor Democraţi, Federaţia Mondială a Oamenilor de Ştiinţă" etc..

Este de la sine înţeles că pentru contracararea unei agresiuni de asemenea proporţii statele occidentale şi-au organizat servicii specializate pe măsură, servicii a căror dominantă doctrinară este preponderent „de acţiune", cum este cazul structurii înfiinţate de preşedintele Herri Trumann în 1948, numită Office off Polyce Coordination, care în 1952 a devenit parte integrantă a C.I.A.. Despre acest organism se ştie precis că are încredinţate trei tipuri de misiuni:

I. Războiul psihologic (propagandă ocultă);

II. Acţiuni politice (contacte şi fonduri secrete necesare pentru a acţiona asupra situaţiei politice dintr-o ţară ostilă sau prietenă, ajungându-se până la diversiune);

III. Operaţiuni militare limitate sau războaie neconvenţionale.

Datorită faptului că dezvoltă o protecţie deosebit de eficientă, organizarea şi multe din acţiunile acestor structuri statale occidentale cu misiuni informative şi contrainformative sunt foarte puţin cunoscute, mai ales în comparaţie cu K.G.B.-ul a cărei activitate a cunoscut un

număr mare de defectori.

Deoarece în democraţie opinia publică se formează pe baza presei, iar liderii nu pot acţiona împotriva curentului opiniei publice, s-a ajuns la situaţia reală, constatată, printre alţii, şi de Michel Rocard că „Puterea mediatică este astăzi mai puternică decât puterea politică”.

Într-o atare situaţie aproape că este inutil să mai precizăm că terenul, câmpul de luptă al războiului mediatic este tocmai opinia publică, prin agresarea conştiinţei fiecărui cetăţean de către colportorii de opinie – recrutaţi din rândul ziariştilor şi al personalităţilor politice, economice, culturale, religioase etc.—, deveniţi vehicule ale dezinformării, vectori ai minciunii.

Deşi minciuna poate îmbrăca mii şi mii de faţete, determinate de cazuistica adusă în discuţie, în esenţă există un număr limitat de „reţete” pentru instrumentarea informaţiei tendenţioase. Spre exemplu, Vladimir Voikoff, în lucrarea Le *Montage* (Paris 1982), considera că „repertoriul minciunii” nu conţine mai mult de zece poziţii.

Cu precizarea că în purtarea războiului mediatic informaţia distorsionată sau total falsă poate căpăta o varietate imensă de nuanţe, în principiu, şi fără a-l considera restrictiv, suntem de acord cu acest „decalog al dezinformării”, care identifică:

1. Abila combinare şi dozare a jumătăţilor de adevăr cu jumătăţi de minciună, primele determinând acceptarea celorlalte şi aceasta cu atât mai uşor cu cât opinia publică este neutră sau deja paralizată.

2. Minciuna absolută, născocirea, adesea eficace datorită enormităţii sale ce poate seduce spiritele paradoxale şi nu numai.

3. Contraadevărul – falsificarea la propriu de documente – neverificabil datorită lipsei de martori.

4. Minciuna prin omisiune, în special aceea care neglijează de a prezenta informaţia în întreg contextul ei, deturnând şi trunchind datele reale.

5. Valorificarea informaţiilor colaterale, a faptului

întâmplător în detrimentul esenţialului, estompat în mod savant.

6. Amestecarea faptelor, a opiniilor sau persoanelor echivalente, care, într-o anumită variantă, vor putea fi plasate cu uşurinţă într-un alt context, eventual incriminate, folosind o ilustrare adecvată, chiar dacă este abuzivă.

7. Recurgerea la informaţii reminiscenţe, indiferent dacă la origine ele au fost reale sau false, pentru a fi puse în contexte diverse sau realiza comparaţii nejustificate.

8. Minciuna înecată într-un noian de informaţii, existând posibilitatea de a fi regăsită ulterior pentru a servi drept punct de referinţă.

9. Citate aproximative sau trunchiate.

10. Forma superioară a minciunii, care înseamnă enunţarea adevărului, dar lâsându-se impresia că este minciună sau negarea unei afirmaţii în aşa fel încât interlocutorul să creadă că, de fapt, o aprobă.

Acestora trebuie să le alăturăm, ca auxiliare, 5 mijloace subtile de dezinformare care, folosind capacitatea persuasivă a limbajului – capabil de nuanţări, ambiguităţi şi inflexiuni –, acţionează asupra auditoriului fără ca acesta să bage de seamă:

1. Afirmaţii făcute pe un ton angelic, dezinvolt sau indignat.

2. Exagerarea apocaliptică a unui fapt colateral, lipsit de importanţă, în numele unor principii morale.

3. Slăbirea adevărului printr-o prezentare sarcastică sau persiflantă.

4. Manipularea abilă a vocabularului prin utilizarea unor termeni imprecişi, meniţi a semăna confuzie, sau a trimite cu gândul la contexte străine subiectului prezentat dar cu conotaţic precisă în opinia publică.

5. Etichetarea interlocutorului atribuindu-i o pretinsă apartenenţă la un anumit sistem de idei, ce deviază atenţia şi poate fi respins mai uşor decât discutarea în detaliu a argumentelor veritabile prezentate.

Dar arsenalul războiului mediatic beneficiază de o

forţă pe cât de veche pe atât de eficientă şi avantajoasă: zvonul. Se poate aprecia că este de neconceput existenţa unui mediu social-politic în care să nu existe zvonuri. Mai mult chiar, politică fără zvonuri nu se face. Zvonul este în esenţă o afirmaţie pe marginea afirmaţiei oficiale. Este o contraputere, motiv pentru care proliferează pe terenul cuceririi gestionării puterii.

Unul dintre cei mai buni analişti contemporani din perspectivă politico-sociologică ai zvonului este Jean-Noel Kapferer. În lucrarea intitulată „Zvonurile – cel mai vechi mijioc de informare din lume" (Paris, 1990; Bucureşti, 1993), acesta avansează următoarea definiţie: „Vom numi aşadar zvon apariţia şi circulaţia în cadrul societăţii a unor informaţii fie încă neconfirmate public de către sursele oficiale, fie dezminţite de acestea. «Se spune» este o «nonspunere», fie că zvonul devansează sursa oficială, fie că o contrazice."

Zvonul evită dezvăluirea identităţii surselor: alţii vorbesc în locul nostru, făcându-se purtătorii vo luntari sau involuntari ai zvonului. Sursa rămâne învăluită îm mister fără;af^putea fi identificată. Nimeni nu-şi asigură responsabilitatea, d;ar^ toţi sunt la curent. Zvonul nu are nevoie de dovezi căci opimitf i publică întemeindu-se mai mult şi de obicei, nu atât pe fapte c:ât^ mai ales pe impresii, acuzaţia este de ajuns.

Aşa cum este ştiut, zvonurile pot li spontane sau i elaborate, reale sau false. Pentru războiul mediatic sunt de luat în considerare cu precădere cele elaborate, care implică véhiculait a neadevărurilor totale sau parţiale. Răspândirea şi dirijarea lor presupune abilităţi speciale, căci trebuie să te fereşti să faci afirmaţi îi tranşante. Se pun întrebări insinuante, păstrând aparenţa de imparţialitate, pentru a determina apariţia îndoielii. Se sugerează ipotoe/^e, lăsând publicului sau interlocutorului direct dreptul de a träges é toncluzii. Se enunţă o enormitate, adăugându-se Imediat că este îânAloieinică dar.... Cine ştie poate...

Este de la sine înţeles că zvonurile sunt

răspânditte^în medii considerate propice, iar difuzarea lor trebuie să se faccă ^asimultan către mai multe ţinte deodată, în aşa fe 1 încât ivirea zwo^tiului din mai multe izvoare să conducă la confirmarea lui.

Alegerea mesajelor este fundamentală, fiind de p^referat o insinuare comportând o parte de adevăr, dar sugerânid * o interpretare peiorativă, defăimătoare. Este indicat să se lanseae^în cadrul unei discuţii între ţinte deoarece, daca va exista un scNhimb de argumente, se vor găsi întotdeauna indivizi care, fie şi n^iumai din spirit de contradicţie sunt gata să susţină veridicitatea. c^alomniei ştirii.

În cadrul zvonului un loc aparte îl ocupă calomnia.. IiAsinuările privitoare la viaţa particulară aduc fntotdeauna folloAase mari deoarece puţini oameni, în afara celoi: apropiaţi vict::iiAiei şi, în consecinţă, suspecţi de părtinire sunt în s tare să dezmintM (Aalomnia. Este de reţinut faptul că avantajul aces-tui gen de operraţ^îii constă în aceea că pune victima în postura de acuzat şi îi impune^ o căutarea de probe pentru dezvinovăţire. Victima trebuie să faiclx i dovada nonexistenţei faptelor incriminate ceea ce este, practic, i Anposibil, având în vedere că prin definiţie, ceea ce nu există nu la-^să urme.

Contrar unei idei răspândite, în viaţa publică nu trebuie niciodată să tratezi calomnia prin dispreţ şi tăcere. Întotdeauna vor exista indivizi bine intenţionaţi capabili să o reînvie la momentul oportun. Adesea, calomnia este o operaţie în doi timpi: mai întâi se aruncă informaţia falsă, fără a părea că i se acordă atenţie, urmând să fie apoi reluată cu referire la prima sa publicare.

Ca mijloc de protecţie şi de neutralizare a calomniei apelul la încredere nu serveşte la nimic, deoarece dezinformatorul se situează de la bun început pe o poziţie favorizantă. De aceea se impune ca fără întârziere să se treacă la contraatac, cerându-se precizări cu privire la faptele incriminate, să fie solicitate dovezi palpabile referitoare la acuzaţie şi originea sa şi, mai ales, să fie deschis un proces de defăimare. Apoi vor trebui declanşate

aceleaşi măsuri împotriva agenţilor de influenţă, indiferent dacă aceştia sunt sau nu complici conştienţi ai dezinformatorului, pentru a-i discredita, intimida şi neutraliza.

Totuşi, în foarte multe cazuri, este dificil să se răspundă unei dezinformări mediatizate. Dezminţirea, chiar dacă este întotdeauna necesară nu este suficientă. După ce şi-a lansat contra-adevărul, mai ales dacă se poate prezenta ca fiind un simplu transmiţător a unei informaţii venite de aiurea, mincinosul nu are altceva de făcut decât să tacă şi să aştepte. Minciuna reprezintă, practic un proces cu trei personaje. În afara „mincinosului" mai există cele două victime ale procedeului: cea asupra căreia acţionează, şi care încearcă fără prea mari şanse de izbândă să facă dovada bunei sale credinţe, şi cea care recepţionează minciuna. Aceasta din urmă, indiferent dacă este o persoană sau însăşi opinia publică, nu are posibilitatea de verificare, situându-se, fără să vrea, în postura unui fel de arbitru, judecător al diferendului ce-l opune pe „mincinos" victimei sale.

Împotriva dezinformării mediatizate nu se poate lupta fără un personal calificat, dispunând de mijloace adecvate şi, în special, fără o direcţie strategică şi tactică care să fixeze scopuri clare şi să coordoneze acţiunile necesare. Aceasta începe, ca în orice alt domeniu, prin identificarea şi cunoaşterea exactă a pericolului.

Că ne place sau nu, războiul mediatic nu mai trebuie tratai superficial. El reprezintă forma vicleană a războiului total şi, chiar dacă regulile pot evolua în funcţie de circumstanţe, se supune unor principii fundamentale ce nu pot fi subestimate fără riscul înfrângerii. Nu este deloc prea mult spus dacă afirmăm că, bine condus, războiul mediatic poate determina capitularea unei naţiuni în eventualitatea unui atac militar sau ideologie, prin pervertirea spiritului, inversarea ierarhiilor socio-culturale locale, reuşite care induc populaţiei o stare de indiferenţă, diminuându-i şi derutându-i capacitatea de înţelegere şi aderenţă la real.

De aceea lupta împotriva dezinformării nu reprezintă un domeniu izolat în care confruntarea se poate desfăşura fără a ţine seama de celelalte imperative ale apărării. Ea poate constitui faza preliminară şi indispensabilă a unor negocieri diplomatice. Poate fi un factor important în reuşita unor tranzacţii economice de amploare. Este o necesitate pentru a putea rezista unei agresiuni psihologice împotriva naţiunii, fie că este vorba de o campanie destinată modelării opiniei publice într-o problemă cheie, fie că vizează degradarea lentă şi progresivă a sistemului de valori recunoscut şi demoralizarea indivizilor.

Orice încercare de apărare în cadrul războiului mediatic trebuie să se desfăşoare în conformitate cu un plan general, care să aibă fixate cu precizie obiectivele şi responsabilităţile. Trebuie refuzate „dep/ano" toate iniţiativele solitare.

De asemenea, apărarea împotriva dezinformării este formal interzisă amatorilor. Prea adesea s-au văzut factori politici responsabili sau comandanţi militari care, crezând că sunt fini psihologi, au fost manevraţi şi depăşiţi de către adversar mult mai competent.

În aceste condiţii trebuie arătată o grijă deosebită formării specialiştilor în domeniu, cerinţă obligatorie şi necesară care solicită timp şi atenţie, precum şi o gândire fără prejudecăţi. Selecţionare de cadre cu însuşiri native, cum ar fi sângele rece, inteligenţa, perspicacitatea, răbdare, subtilitate etc., etc., care vor trebui să înveţe şi să-şi însuşească numeroase cunoştinţe din domenii foarte diverse, în baza unei bune programe de instruire şi a studiului aprofundat. Neapărat, aceşti specialişti vor trebui să acumuleze o experienţă practică, însă fără a pune în pericol, prin încercări intempestive, societatea pe care sunt chemaţi să o protejeze.

Nu trebuie scăpat din vedere faptul că în domeniul războiului mediatic orice acţiune, inclusiv aceea de a pregăti şi forma un personal specializat, constituie un act de război şi poate determina o contra-acţiune inamică. În

plus trebuie adăugat faptul că într-o societate deschisă cum este a noastră vor exista întotdeauna spiritele nobile – în sensul pur al cuvântului – sau naivi care să denunţe cu vehemenţă însăşi existent războiului mediatic, a luptei psihologice. Sensibilizarea, pregătirea şi informarea prealabilă a publicului sunt indispensabile oricărei acţiuni. Aceste misiuni aparţin celor care guvernează şi mijioacele de informare în masă care trebuie, în primul rând, convinse.

Pentru reuşita în lupta de neutralizare a războiului mediatic un factor esenţial îl reprezintă conştiinţa fiecărui cetăţean. Aceştia nu pot rămâne simpli spectatori, aşa cum ar fi posibil, la nevoie, în situaţia confruntărilor cu caracter militar sau economic. Este vorba de un domeniu în care „consensul”, adesea invocat, însă rareori realizat, reprezintă un imperativ naţional absolut. Apărarea împotriva dezinformării nu se va putea realiza fără participarea generală a celor ce-i sunt victime. Imposibilitatea de a mai încredinţa altora grija pentru securitatea proprie constituie pentru cetăţenii noştri o situaţie nouă, căreia nu-i vor putea face faţă de pe o zi pe alta.

„Consensul” naţional este, în mare măsură, determinat de încrederea pe care cetăţenii o acordă statului ce-i guvernează. În acest context, trebuie să constatăm că micile şiretlicuri folosite în politica internă, cărora niciun guvern democratic din nicio ţară nu le poate rezista, riscă să coste foarte scump naţiunea pe planul apărării moralului. Încrederea nu este un capital din care să sc poată consuma la cerere: ea exista sau nu. În democraţii, toţi indivizii obişnuiţi vor trebui să înveţe ce este aceea francheţe şi loialitate dacă vor să supravieţuiască.

Această necesară sporire a moralităţii vieţii politice democrate ar putea fi una dintre consecinţele neaşteptate ale războiului mediatic. Căci ne putem pune problema care va fi evoluţia raportului de forţe dintre regimurile care practică o obiectivitate reală, deci urmate clar de

popoarele lor, şi cele ce se vor încăpăţâna să continue a trişa cu ideile şi faptele. Minciuna guvernanţilor va duce cel mult la pasivitatea supuşilor şi la reticenţa executanţilor, ceea ce nu facilitează deloc confruntarea cu realităţile lumii. Originalitatea războiului mediatic constă tocmai în faptul că atitudinea de sinceritate nu este determinată de cauze etice, ci de realism şi necesitate.

6. RĂZBOIUL ELECTRONIC

Impactul mediului electromagnetic asupra capabilităţii operaţionale a forţelor militare, echipamentelor, sistemelor şi platformelor este atribuit efectelor mediului electromagnetic, care cuprinde toate disciplinele electromagnetice, precum compatibilitatea şi interferenţa electromagnetică, protecţia electronică, riscurile radiaţiei electromagnetice asupra mijioacelor şi materialelor volatile, precum şi efectele fenomenelor naturale – fulgerul şi precipitaţiile. Echipamentele şi sistemele care operează pe principiile electromagnetismului sunt caracterizate de vulnerabilitatea electromagnetică care le cauzează incapacitatea de a îndeplini misiunea stabilită, ca urmare a efectelor mediului electromagnetic.

În operaţiile militare, termenul de război electronic *cuprinde ansamblul acţiunilor militare care implică utilizarea energiei electromagnetice pentru a determina, exploata, contracara, reduce şi preveni acţiunile ostile în spaţiul electromagnetic, precum fi măsurile care asigură desfăşurarea în siguranţă a trupelor proprii şi/sau aliate*.

Războiul electronic are trei componente principale: atacul electronic, protecţia electronică şi sprijinul electronic.

Atacul electronic. Atacul electronic este componenta războiului electronic care implică utilizarea energiei electromagnetice, a energiei dirijate sau a armelor antiradiaţie pentru a ataca mijloacele, echipamentele sau personalul, cu intenţia de a degrada, neutraliza sau distruge capabilităţile de luptă ale inamicului ci este considerată o formă de luptă. Atacul electronic include:

acţiunile întreprinse pentru a preveni sau reduce utilizarea cu eficienţă de către inamic a spectrului electromagnetic, cum ar fi bruiajul şi înşelarea electronică;

— utilizarea armelor care folosesc energia electromagnetică sau energia dirijată ca principal mecanism distructiv (lasen, arme dirijate pe fasciculul de radiofrecvenţă sau fascicule de particule cu energie înaltă).

Protecţia electronică. Protecţia electronică este o componentă a războiului electronic care implică aplicarea de măsuri active şi pasive pentru protecţia personalului, mijloacelor şi echipamentelor la efectele utilizării războiului electronic de către forţele proprii sau inamice.

— Sprijinul electronic. Sprijinul electronic este componenta războiului electronic implicată în acţiunile întreprinse pentru a căuta, intercepta, identifica şi localiza sursele de radiaţie intenţionată sau neintenţionată a energiei electromagnetice, în scopul recunoaşterii imediate a unei ameninţări, combaterii acesteia, planificării şi conducerii operaţiilor viitoare. Sprijinul electronic asigură informaţiile necesare luării deciziei de implicare a războiului electronic în operaţii sau alte acţiuni tactice cum ar fi evitarea ameninţării, stabilirea ţintelor şi dirijarea. Datele de sprijin electronic pot fi utilizate pentru a furniza informaţii privind semnale (*SIGINT*), pentru stabilirea ţintelor atacului electronic sau pentru distrugerea fizică şi pentru măsurarea parametrilor şi determinarea amprentei semnalelor (*MASINT*). SIGINT poate contribui la estimarea rezultatelor atacului şi pe această bază, la modificarea planului operaţional general.

Acţiunile de război electronic sunt executate în tot spectrul electromagnetic pentru a asigura şi menţine controlul şi utilizarea eficientă a acestuia de către forţele proprii şi pentru a interzice utilizarea lui de către forţele inamicului prin modificare, distrugere, întrerupere sau înşelare. Necesitatea controlului spectrului electromagnetic şi tipul de acţiuni de război electronic necesare pentru controlul acestuia sunt dictate de mediul

operaţional în care se desfăşoară acţiunile militare.

Loc şi rol

Principalul rol al acţiunilor de război electronic este de a câştiga confruntarea în spaţiul electromagnetic cu sistemele electronice a căror activitate poate fi, după caz, potenţial ostilă sau ostilă.

Pe *timp de pace*, rolul războiului electronic este de a identifica şi dimensiona factorii de risc şi ameninţările la adresa securităţii şi apărării naţionale, specifice spaţiului electromagnetic, precum şi realizarea unei capacităţi de descurajare şi reacţie credibilă, adecvată tuturor situaţiilor probabile.

În situaţii de criză, rolul războiului electronic este de a supraveghea spaţiul electromagnetic din zonele de crize, în cooperare cu celelalte forţe implicate pentru gestionarea şi rezolvarea acestora.

La război, rolul războiului electronic este de a diminua potenţialul de luptă inamic concomitent cu multiplicarea capacităţilor de acţiune a forţelor proprii prin câştigarea confruntării în spaţiul electromagnetic, conform concepţiei operaţiei.

În operaţiile întrunite, războiul electronic reprezintă una din capabilităţile militare care sunt integrate în operaţiile informaţionale.,

Deoarece poate afecta colectarea, procesarea, păstrarea şi transmiterea informaţiilor bazate pe energia electromagnetică, războiul electronic reprezintă o componentă esenţială a operaţiei informaţionale. Războiul electronic are, de asemenea, un rol important în suprimarea apărării antiaeriene a inamicului (*SEAD*).

Acţiunile principale de război electronic

Principalele acţiuni de război electronic au apărut de-a lungul timpului pentru a exploata oprtunităţile şi vulnerabilităţile inerente în fizica energiei electromagnetice. În acest sens continuă dezvoltarea de noi echipamente şi tactici, deşi fizica energiei electromagnetice rămâne constantă. Aceasta este raţiunea pentru care acţiunile de bază ale războiului electronic

rămân eficace în pofida schimbării echipamentelor şi tacticilor.

Principalele acţiuni desfăşurate în cadrul războiului electronic sunt:

6.1. Compatibilitatea electromagnetică

Compatibilitatea electromagnetică (*EMC*) reprezintă capabilitatea sistemelor, echipamentelor şi componentelor care utilizează spectrul electromagnetic de a funcţiona în mediile operaţionale destinate fără a suferi sau produce degradări inacceptabile din cauza radiaţiei sau reflexiei electromagnetice. Compatibilitatea electromagnetică implică: aplicarea strictă a gestionării spectrului electromagnetic; proiectarea sistemelor, echipamentelor şi componentelor care să asigure funcţionarea acestora fără interferenţe; concepte şi doctrine clare care să crească eficienţa operaţională.

6.2. Dezinformarea electronică

Dezinformarea electronică reprezintă radierea deliberată, reradierea, denaturarea, suprimarea, absorbţia, interzicerea, amplificarea sau reflexia energiei electromagnetice în mod intenţionat pentru a induce în eroare inamicul sau sistemele de arme ale acestuia, care utilizează energia electromagnetică, având drept consecinţă diminuarea sau neutralizarea capabilităţilor de luptă ale inamicului. Dezinformarea electronică se prezintă sub următoarele forme:

— Dezinformarea electronică manipulativă. Acest tip de dezinformare implică acţiuni de eliminare a indiciilor de demascare relevanţi care pot fi utilizaţi de către inamic, precum şi transmiterea unor indicii false.

— Dezinformarea electronică simulativă. Acest tip de dezinformare implică acţiuni de simulare a capabilităţilor forţelor şi mijloacelor proprii pentru a induce în eroare forţele inamicului.

Dezinformarea electronică imitativă. Acest tip de dezinformare induce energie electromagnetică în sistemele electronice ale inamicului care imită emisiile acestuia.

6.3. Robustizarea electromagnetică

Robustizarea electromagnetică constă în acţiunile întreprinse pentru protejarea personalului, echipamentelor şi infrastructurii împotriva efectelor nedorite ale energiei electromagnetice, prin filtrare, atenuare, împământare şi ecranare.

6.4. Interferenţa electromagnetică

Interferenţa electromagnetică (EMI) reprezintă orice perturbare care întrerupe, obstrucţionează, modifică sau limitează performanţele echipamentelor electrice sau electronice. Aceste perturbaţii pot fi induse intenţionat ca în forme ale războiului electronic sau neintenţionat, ca urmare a emisiilor secundare, precum şi ca urmare a fenomenului de intermodulaţie.

6.5. Penetrarea electromagnetică

Penetrarea electromagnetică reprezintă introducerea intenţionată prin diferite metode a energiei electromagnetice în calea de transmitere, în scopul inducerii în eroare a operatorilor sau pentru a provoca confuzie.

6.6. Bruiajul electronic

Bruiajul electronic reprezintă radiaţia deliberată, reradiaţia sau reflectarea energiei electromagnetice pentru a preveni sau reduce folosirea eficientă a spectrului electromagnetic de către inamic în scopul diminuării sau neutralizării capabilităţilor de luptă ale inamicului.

6.7. Impulsul electromagnetic

Impulsul electromagnetic reprezintă un impuls foarte puternic cauzat cel mai adesea de o explozie nucleară care afectează sistemele electrice şi electronice, producând defectarea acestora prin intensitatea mare a curentului indus şi supravoltaj.

6.8. Mascarea electronică

Mascarea electronică reprezintă radiaţia controlată a energiei electromagnetice pe frecvenţele proprii astfel încât să se asigure protecţia emisiilor proprii împotriva măsurilor de sprijin electronic sau SIGINT ale inamicului, fără a afecta semnificativ lucrul sistemelor proprii.

6.9. Stimularea electronică

Stimularea electronică reprezintă radiaţia intenţionată destinată a fi indusă în sistemele şi componentele electronice ale potenţialului inamic pentru a le determina să reacţioneze, cu scopul de a cunoaşte capabilităţile operaţionale şi acţionale ale acestora.

6.10. Recunoaşterea electronică

Recunoaşterea electronică reprezintă descoperirea, localizarea, identificarea şi evaluarea radiaţiilor electromagnetice.

6.11. Cercetarea electronică

Cercetarea electronică (ELINT) reprezintă cercetarea tehnică şi localizarea radiaţiilor electromagnetice noncomunicaţii emise de alte surse decât exploziile nucleare sau radioactive.

6.12. Securitatea electronică

Securitatea electronică reprezintă protecţia rezultată ca urmare a aplicării tuturor măsurilor destinate interzicerii accesului persoanelor neautorizate la informaţii de valoare, prin interceptarea şi studierea radiaţiilor electromagnetice noncomunicaţii.

6.13. Reprogramarea acţiunilor de război electronic

Reprogramarea acţiunilor de război electronic reprezintă schimbarea sau modificarea intenţionată a acţiunilor de război electronic sau a sistemelor de senzori ca răspuns la schimbările produse în mediul electromagnetic, echipamente şi tactici. Aceste schimbări pot fi rezultat al acţiunii deliberate a forţelor proprii, inamicului sau a unei terţe părţi, ori pot fi determinate de interferenţa electromagnetică sau alte fenomene aleatoare. Scopul reprogramării acţiunilor de război electronic este acela de a menţine sau îmbunătăţi eficacitatea acţiunilor de război electronic şi a echipamentelor sistemelor de senzori. Reprogramarea acţiunilor de război electronic include schimbările din sistemele de auto apărare, sistemele de arme ofensive şi sistemele de informaţii.

6.14. Controlul emisiei

Controlul emisiei (*EMCON*) reprezintă utilizarea

selectivă şi controlată a emiţătorilor electromagnetici, acustici sau de altă natura, în scopul optimizării capabilităţilor de comandă şi control

(C2), simultan cu minimizarea, în folosul securităţii operaţiilor a:

detectării de către senzorii inamicului;

interferenţei reciproce între sistemele proprii;

factorilor care împiedică executarea planurilor proprii de dezinformare militară.

6.15. Gestionarea spectrului

Gestionarea spectrului implică planificarea, coordonarea şi administrarea utilizării spectrului electromagnetic prin proceduri operaţionale, administrative şi tehnice. Obiectivul gestionării spectrului electromagnetic este de a permite sistemelor electronice să lucreze la posibilităţile maxime în mediul dat, fără a produce sau suferi interferenţe inacceptabile.

6.16. Regimuri de lucru de rezervă

Regimurile de lucru de rezervă (*WARM*) reprezintă caracteristicile şi procedurile de operare ale senzorilor, sistemelor de comunicaţii, navigaţie, recunoaştere, a celor de arme, precum şi a sistemelor de contraacţiune, care vor contribui la creşterea eficacităţii acţiunilor militare dacă nu sunt cunoscute sau înţelese de către inamic înainte de a fi utilizate, dar care pot fi exploatate sau neutralizate dacă sunt cunoscute anterior. Regimurile de lucru de rezervă sunt păstrate în mod intenţionat în rezervă pentru situaţii de criză sau în caz de război.

Aşadar, având în vedere că în prezent mijloacele electronice sunt utilizate atât de organizaţiile militare cât şi de cele civile pentru comunicaţii, navigaţie, ca senzori, pentru păstrarea şi prelucrarea informaţiilor, putem concluziona că utilizarea mediului electromagnetic crează vulnerabilităţi şi oportunităţi pentru războiul electronic, iar forţele armate fac tot posibilul pentru a profita de acest aspect în sprijinul operaţiilor militare.

7. TERORISMUL INFORMATIC

Terorismul informaţional se poate defini în contextul

războiului informaţional, cât şi într-acela al terorismului convenţional.

Într-un efort de a atrage atenţia publicului, teroriştii politici îşi săvârşesc propriile acte utilizând mijloacele de informare în prim planul strategiilor lor, bazându-se pe presupunerea că accesul la structura de comunicaţii este legat de putere. Cei care cred în această presupunere ar putea viza sistemele informaţionale digitale în urmărirea obiectivelor politice.

Infrastructura informaţională sprijină transferurile de informaţii militare, financiare şi comerciale de către consumatori sau în interesul unor state. Luând în considerare prezenţa computerului în societatea modernă, nu este surprinzător că în trçcut teroriştii au vizat uneori sistemele de computere, în Japonia unele grupuri au atacat sistemele de control computerizat al trenurilor de navetişti, paralizând câteva ore cele mai importante oraşe; manifestul Brigăzii Roşii italiene stipula că distrugerea instalaţiilor şi a sistemelor de computere reprezenta un obiectiv pentru „a lovi în inima statului”. Mai recent, suporterii Sinn Fein de la Universitatea Austin din Texas au expus pe Internet detalii sensibile despre instalaţii ale serviciilor militare de informaţii britanice şi despre secţii de poliţie din Iranda de Nord.

[*Pe măsură ce tehnologia devine tot mai accesibilă, disponibilitatea şi potenţialul acesteia cresc, în timp ce costurile financiare şi celelalte costuri scad, teroriştii putând deveni mai orientaţi pe tehnologie în tacticile şi strategiile lor. Cele mai vulnerabile la a fi atacate sunt sistemele automatizate, cele care depind într-o mare măsură de ultimele tehnologii, avansul tehnologic prezentând dezavantajul că, în eventualitatea în care o tehnologie conţine greşeli de proiectare, pagubele rezultate sunt direct proporţional cu valoarea respectivei tehnologii. În acelaşi timp trebuie avut în vedere că pe măsură ce un sistem este tot mai complex, posibilităţile de apariţie a unor erori cresc.*]

Avioanele comerciale, conductele de gaz natural,

reţeaua de energie electrică, platformele marine de foraj, precum şi înregistrările de date de pe sistemele de stocare ale organizaţiilor guvernamentale sau ale anumitor corporaţii reprezintă exemple de obiective expuse sabotajului, ale căror distrugeri ar avea efecte implicite de intensitate mult mai mare decât pierderile principale pe care acestea le-ar putea sugera...

În prezent, mai degrabă decât să atace un anumit obiectiv bine protejat sau să încerce operaţiuni care să implice rezultate cu grad (potenţial) ridicat de risc, teroriştii vor căuta şi vor exploata vulnerabilităţi încă neidentificate până acum şi, pur şi simplu, îşi vor adapta corespunzător planul de atac şi priorităţile tactice.

Includerea tehnologiei informaţiei în cadrul complexului militaro-industrial, precum şi proiectarea şi implementarea strategiilor de război informaţional pot, de asemenea, să atragă teroriştii spre utilizarea tehnologiei computerelor.

[*în prezent, în cazul României, riscurile expunerii la eventuale atacuri ale unor terorişti informaţionali sunt scăzute, datorită „avantajului" oferit de inexistenţa unor sisteme integrale care să rezolve funcţiuni vitale, de interes naţional şi, probabil, datorită dezinteresului prezentat de cyberspaţiul autohton*.]

Se încearcă, în continuare să se ofere o definiţie a terorismului informaţional, plecând de la definirea războiului informaţional. Un act de violenţă politică, exercitat de către oricine altcineva decât un membru al unor forţe armate ale unui stat legitim, este tratat adesea drept un act de terorism. Această abordare este, însă, doar rareori corectă, dar conotaţia subversivă şi criminală a termenului „terorist" a reieşit şi din multe acţiuni în care s-a abuzat de utilizarea computerelor, acestea fiind etichetate drept „terorism informaţional".

Politica şi metodologia de contracarare a acestor acte criminale depinde într-o mare măsură de motivaţiile făptuitorilor; prin urmare sunt necesare definiţii mai clare şi mai concise asupra „terorismului informaţional", dacă

acesta trebuie să fie luat în calcul de către politica de securitate naţională.

Terorismul politic reprezintă folosirea sistematică a violenţei fizice actuale sau care se întrevede pentru atingerea unui obiectiv politic, pentru a crea un climat general de teamă publică şi de destabilizare a societăţii, influenţând astfel populaţia sau politica guvernamentală.

Terorismul informaţional reprezintă legătura dintre acţiunile criminale de abuz sau fraudare a sistemelor informaţionale şi violenţa fizică a terorismului. Prin urmare, în special din punct de vedere legal, terorismul informaţional poate fi reprezentat de utilizarea abuzivă a sistemelor informatice digitale, reţelelor sau a altor componente pentru un rezultat final care sprijină sau facilitează o acţiune sau campanie teroristă.

Următoarea încercare de împărţire a tipurilor de terorism informaţional vizează mijioacele şi obiectivele urmărite de acesta. Exista două metode generale prin care un terorist ar putea desfăşura un atac informaţional terorist: atunci când este vizată tehnologia informaţiei, şi / sau când tehnologia informaţiei reprezintă mijlocul prin care se realizează o operaţie mai largă.

Prima metodă se referă la faptul că un terorist ar putea viza un sistem informatic în vederea sabotării, fie aceasta fizică sau electronică, aşadar distrugând sau afectând chiar sistemul informatic şi orice infrastructură informaţională (de exemplu, surse de energie electrică, comunicaţii etc.) în funcţie de tehnologia vizată.

Cea de a doua metodă se referă la faptul că un terorist ar putea manipula şi exploata un sistem informatic, prin alterarea sau furtul de date sau prin forţarea sistemului pentru îndeplinirea de către acesta a unor funcţii pentru care acesta nu a fost destinat (de exemplu, utilizarea ilegală a unor mijloace de control aerian).

Pentru o mai bună înţelegere a conceptelor terorismului informatic vom prezenta un studiu de caz (un scenariu) asupra unor evenimente legate de tensiunile

declanşate de sârbii bosniaci pe fondul nemulţumirii provocate de tratamentul discriminatoriu al Statelor Unite şi NATO faţă de sârbii bosniaci şi croaţi.

Ca urmare a nemulţumirilor existente de partea sârbă s-a format un grup paramilitar de sârbi din Bosnia, Serbia şi din alte părţi, intitulat „Consiliul Sârb pentru Eliberarea Bosniei” (SCLiB), cu influenţă politică şi militară printre oficialii sârbi din Bosnia şi din Yugoslavia; de asemenea, Consiliul este format din studenţi sârbi din Slovenia, Ungaria şi Yugoslavia şi a început să-şi sporească efectivele o dată ce membrii săi au început să comunice şi să se întâlnească prin intermediul Intemet-ului, utilizând criptarea mesajelor pentru a-şi ascunde intenţiile şi interesele.

[*Reiese de aici posibilitatea ca grupuri de indivizi să poată comunica în condiţii destul de sigure prin intermediul mesajelor criptate transmise prin poşta electronică*.]

Principalul lor obiectiv este răzbunarea, pentru alungarea mâhnirii provocate de ocuparea teritoriilor de către croaţi, împotriva ajutorului oferit de „stăpânii lor americani” şi pentru îndepărtarea prezenţei NATO din zonă prin dramatizarea cauzei lor în faţa cetăţenilor întregii lumi, influenţându-i pe aceştia şi, astfel, guvenele statelor cărora le aparţin, pentru a cere NATO să părăsească zona.

A fost provocată ciocnirea a 2 avioane C-130, în accident pierind toţi membrii echipajelor ambelor avioane. Imediat după reuşita atentatului au fost anunţaţi prin telefonul celular organizatorii, aflaţi în Slovenia, care au lansat imediat un „comunicat electronic”, asumându-şi responsabilitatea incidentului şi prezentându-şi manifestul şi revendicările. Era indicată adresa de accesare a site-ului lor Web care era ruiat de pe un computer din Amsterdam de către studenţi sloveni, prin intermediul unui cont „anonymous” din Finlanda. Acest mesaj a fost trimis către fiecare organizaţie importantă de ştiri electronice şi tipărite din lumea industrializată.

[*Este un scenariu perfect plauzibil şi potenţial spre a fi aplicat într-o situaţie asemănătoare pe vreun aeroport din ţară, dacă ar exista o grupare locală suficient de bine înzestrată financiar şi logistic şi suficient de motivată pentru atingerea unui asemenea scop*].

Conţinutul acestei pagini de Web era dramatic şi plin de elemente de propagandă şi revendicări împotriva americanilor, a NATO şi a atrocităţilor şi imperialismului croat în regiunea balcanică şi conţinea afirmaţii nefondate asupra unor transferuri ilegale de arme între organisme ale NATO şi croaţii sau musulmanii bosniaci. Au fost introduse câteva referinţe asupra prezenţei anterioare a americanilor în Liban şi asupra modului în care a fost rezolvată această prezenţă.

Publicitatea rezultată este uluitoare: CNN, Reuters, ITAR-TASS şi AP au difuzat imediat mesajul împreună eu adresa Web. La şase minute dupa primirea comunicatului electronic pagina de Web a

Consiliului a fost apelată pentru prima dată. La 24 de ore după atentat, pagina de Web a Consiliului primise peste un milion de apeluri.

[*Transmiterea simultană a „comunicatului" prin intermediul poştei electronice la principalele agenţii de presă a contribuit decisiv la amploarea publicităţii create în jurul atentatului*]

La 24 de ore după prima accesare, primul sistem de pe care s-a realizat accesul a „crăpat", iar toate fişierele au fost şterse fără vreo posibilitate de recuperare, ca rezultat a unui program care se activa după 24 de ore, pe care hackerii Consiliului l-au inclus în conţinutul paginii Web accesate, exploatând anumite defecte din limbajele de programare.

Deşi acesta a creat un climat senzaţional de teamă în întreaga lume a utilizatorilor obişnuiţi de computere, cea mai mare pagubă a fost produsă organizaţiilor de investigaţii şi acelora ale apărării care au accesat imediat şi, în mod natural, pagina de Web înainte ca organizaţiile de ştiri să o răspândească. Printre aceste organizaţii s-au

numărat Departamentul American al Apărării, ministerele apărării ale tuturor ţărilor membre NATO, Departamentul Justiţiei, Departamentul Finanţelor şi Agenţia Centrală de Informaţii. Pagubele finale produse sistemelor nesecrete a fost incalculabil, dar dramatizarea cauzei Consiliului a fost cu adevărat eficientă.

[*Este interesantă intenţia teroriştilor de a spori interesul asupra evenimentului şi de a întări impresia publicului asupra ineficienţei acţiunilor autorităţilor prin distrugerea datelor conţinute pe calculatoarele care au accesat pagina de Web, prin aceasta reuşind să accentueze tensiunea provocată de atentat.*]

Rapoartele asupra atentatului au ajuns la public împreună cu teama creată de dezastrele produse asupra computerelor şi frustrarea generală asupra eforturilor americane în Balcani, creând o presiune enormă asupra Congresului şi a Preşedintelui. Cu alegeri pentru Congres abia peste o lună, incidentul a devenit un punct de concentrare a presiunii congresmenilor asupra Preşedintelui, care a cedat în cele din urmă, în faţa cererilor publicului şi Congresului de aducere acasă a trupelor americane.

[*Organizarea atentatului a fost destul de minuţioasă, având în vedere obţinerea rezultatelor scontate, precum şi asigurarea integrităţii făptuitorilor prin studierea legislaţiei celor două state, Olanda şi Finlanda. Trebuie scoasă în evidenţă lipsa legislaţiei române în cazul unor astfel de infracţiuni.*]

Datorită lipsei unui tratat, agenţiilor americane de investigaţii nu le-a fost permis să violeze protocoalele „cyber-comunităţii" finlandeze; aşadar, investigatorii nu au putut să stabilească identitatea clientului serverului anonymous sau să localizeze poziţia site-ului Web din Amsterdam. Teroriştii informatici ai Consiliului au rămas în anonimitate în siguranţă, iar succesul lor în a se ascunde a determinat apariţia mai multor pagini Web, „clone" ale celei originale a teroriştilor, apariţia unei multitudini de „eliberatori ai Internet-ului" şi reeiFCularea manifestului

original al Consiliului şi a altor detalii prezente în pagina de Web a acestora.

[*Teroriştii şi-au atins cu claritate şi eficienţă obiectivul strategic*.]

Se pune acum problema posibilităţilor de răspuns ale autorităţilor, plecând de la premisa că într-o societate democratică o dilemă în combaterea terorismului este reprezentată de găsirea unei echilibrări corecte între asigurarea drepturilor şi a securităţii civile. Operaţiunile militare într-o societate democratică, chiar dacă sunt destinate „protecţiei" acesteia, sunt adesea în discordanţă cu principiile acelei societăţi. Militarii se confruntă cu un paradox: deşi teroriştii pot folosi forţa brutală, nediscriminatorie faţă de civili sau militari, răspunsul militar trebuie să fie limitat şi numai dacă făptuitorul unui act terorist este găsit ca fiind sponsorizat de către un anumit stat, este posibil un răspuns militar împotriva statului respectiv.

Guvernul Statelor Unite s-a lovit de un asemenea paradox cu ocazia confruntării cu terorismul informaţional. Bazele de date, sistemele de computere, infrastructurile informatice militare, comerciale şi civile în totalitate reprezintă obiective potenţiale ale teroriştilor informaţionali. Indiferent dacă prin intermediul unor mijioace fizice sau digitale, teroriştii informaţionali pot distruge, afecta, degrada, interzice sau întârzia accesul la informaţiile vitale pe care se bazează militarii şi, astfel, putând deveni o ameninţare în timp de pace, la fel de bine ca şi pe timpul războiului.

[*Se atrage atenţia asupra dificultăţilor ivite atunci când trebuie răspuns unor asemenea acte teroriste şi asupra nivelului ameninţării prezentate de astfel de atacuri*.]

Întotdeauna militarii vor constitui ţinta teroriştilor informaţionali. Mai mult, atacurile teroriştilor informaţionali pot fi sponsorizate de un anumit stat şi pot reprezenta prima undă a unui „Pearl Harbour digital". Originea atacurilor digitale este, în general, dificil de

descoperit încă de la primul dintre acestea şi în cazul în care atacul este într-adevăr, un precursor al unui război informaţional dintre două state va fi necesar un răspuns militar.

Aşadar, societăţile democratice trebuie să evalueze cu grijă utilizarea forţelor militare pentru prevenirea şi contracararea terorismului, chiar şi în cazul în care militarii lor pot constitui ţinta acestor atacuri. Prin determinarea militarilor să ofere un răspuns la acţiunile teroriste convenţionale, teroriştii şi cauza acestora pot căpăta un anumit grad de legitimitate. Ulterior acţiunile teroriste pot fi escaladate de la un nivel criminal la acela de „inamic al statului". Acest impas poate fi eliminat atunci când se iau contramăsuri teroriste.

[*Se sugerează ca răspunsurile date unor asemenea atacuri să fie „anonimerapide şi pe deplin corelate eu potenţialul atacatorilor. Se recomandă alcătuirea unor echipe mixte, formate din militari şi din membri ai organizaţiilor de supraveghere a respectării legilor. Din punctul de vedere al atribuţiilor, o astfel de structură poate să conţină militari cu un rol consultativ în cazul incidentelor obişnuite şi, spre deosebire de acest caz, elemente de la agenţiile de supraveghere a respèctării legilor cu un rol consultativ în cazul unor incidente externe.*]

Tehnicile ofensive de război informaţional dezvoltate spre a fi utilizate de către militari la nivel de stat pot fi utilizate, de asemenea, pentru a răspunde terorismului informaţional. În general, agenţiile de supraveghere a respectării legilor nu dispun de posibilităţi asemănătoare pentru ducerea unui război informaţional.

[*Se prezintă necesitatea existenţei unui grup specializat şi integrat pentru a lupta împotriva terorismului informaţional. Astfel de „Echipe de Răspuns Digital Integrat" vor lucra de la sisteme informatice conectate de la distanţă şi vor utiliza tactici de război informaţional pentru a detecta, localiza şi contracara teroriştii informaţionali. Membrii acestora vor trebui*

organizaţi în celule aflate la distanţă, vor exploata elementele de resortul tehnologiei informaţiilor; capacităţile de în vestigaţii şi mijloacele de informaţii ale agenţiilor de supraveghere a respectării legilor. Aceşti luptători informaţionali, formaţi din membri de la mai multe arme (*specialităţi*), *ca şi din membri ai Departamentelor Justiţiei şi Finanţelor vor lovi utilizând mijloace digitale computerele şi reţelele utilizate de teroriştii informatici. Folosind un răspuns anonim, instituţiile guvernamentale pot lovi teroriştii informaţionali fără a se afişa sau legitima, întrucât ambele pot conduce la răspunsuri fizice din partea acestora. Un astfel de răspuns oferă ultima dezminţire plauzibilă. Această structură ar putea combina elementele de investigaţii şi cele jurisdicţionale aparţinând comunităţii care asigură respectarea legilor, cu posibilităţile ofensive ale militarilor.*]

Posibilităţile noastre ofensive îndreptate împotriva unor competitori egali sau aproape egali sunt formidabile, indiferent dacă este cazul războiului informaţional sau a celui convenţional. Aşadar, integrarea elementelor agenţiilor de supraveghere a respectării legilor este necesară pentru a răspunde eficient la un atac dintr-o reţea dintr-o zonă gri.

[*Este ilustrată astfel necesitatea existenţei unei politici integrale, cu un răspuns pe deplin formulat, care să acopere spectrul ameninţărilor bazate pe informaţii la adresa securităţii naţionale, care să conducă elementele de ofensivă şi apărare ce pot răspunde simetric şi eficient.*]

Deocamdată, România se găseşte încă departe de riscurile unor asemenea ameninţări, plecând, în special de la premisa inexistenţei unei infrastructuri generale adecvate, dar asemenea ameninţări pot ajuta mult la pregătirea unor măsuri de protecţie pentru cazul în care vom *fi* în măsură să dispunem de ceva de apărat în acest domeniu. Mult mai aproape de realitate este problema supravegherii cetăţenilor romani care, mai degrabă dezorganizat, sunt în măsură să realizeze atacuri asupra

unor sisteme informatice din afara ţării (acte considerate de legislaţia majorităţii statelor respective drept „terorism informaţional”) şi, deci, mai în măsură să afecteze imaginea publică şi interesele statului român.

ANEXA 3

Resurse URL (Uniform Resourse Locator)

Operaţii informaţionale – în general http://www.afcea.org şi http://www.us.net/signal/

AFCEA publică regulat articole despre operaţiile informaţionale, intelligence şi C2 în publicaţia lor lunară Signal.

http://www.aracnet.com/~gtr/archive/infowar.html Bibliografia lui K. Anderson despre războiul informaţional şi documente despre vulnerabilitatea infrastructurilor.

http://huachuca-usaic.armv.mil/

Centrul de Intelligence al Armatei SUA: publicaţii şi doctrine. http://www. aipio. asn. au/links. htm

Resurse URL australiene cu legături la multe resurse de intelligence din lume.

http://www.dodccrp.org/bostoc.htm

Lecţii din Bosnia: Experienţa IFOR (carte disponibilă electronic) http://www.dodcerp.org

Programul de Cercetare Cooperativă C4ISR al Departamentului Apărării SUA şi resursele Războiului Centrat pe Reţele http://www.ndu.edu/inss/books/diw/index.html

Războiul Informaţional Defensiv publicaţie a Universităţii

Naţionale a Apărării (NDU) a SUA

http://www.jva.com

Website actualizat zilnic cu articole internaţionale şi ştiri în domeniul criptografiei, războiului informaţional, nivelul de comandă şi intelligence-ului http://www.rand.org/publications/MR/MR880/contents.html În Athena's Camp: Pregătirea pentru conflict în Era Informaţională. John Arquila şi David Ronfeldt.

http://www.ndu.edu/inss/siws/cont.html

Sun Tuz, Arta Războiului în Războiul Informaţional,

carte electronică cu o colecţie de articole.

http://www.infowar.com

Site-ul Winn Schwartau despre războiul informaţional şi securitate cu multe legături şi articole.

http://www.infomatik.umu.se/~rhwit/IW.html

Paginile de război informaţional ale lui Randy Whitaker de la

Universitatea Suedeză Umea.

Resurse pentru operaţii informaţionale http.y/www.tno.nl/instit/fel/infoops

Resurse URL ale TNO-FEL despre Operaţii Informaţionale, Siguranţă Informaţională, Securitate Informaţională.

http://www.psvcom.net/war. 1.html

Institutul pentru studii avansate de război informaţional (IASIW).

http://www.twurled-world.com/Infowar/Update2/ cover.htm Vedere de ansamblu a resurselor de război informaţional din lumea întreagă bazată pe analiză de scanare web.

http://cryptome.org/fm 1 OO/fm 100-6.htm

Manual de teren 100-6: operaţii informaţionale.

http: //www. dtic. mi l/doctrine/j el/cpub s2. htm

JS Join Publication 3-13: Doctrina Integrată pentru Operaţii

Informaţionale, 9 octombrie 1998; JS Join Publication 3-54:

Doctrina Integrată pentru Operaţii de Securitate, 24 ianuarie 1997.

http://www.dtic.mil/doctrine/jv2020/jvpub.htm JSJoin Vision 2020

Aspecte legale ale Operaţiilor Informaţionale http://www.usdoj.gov/criminaiycybcrcrimc Departamentul de Justiţie al SUA pentru Infracţiuni prin Calculator şi Drepturi de Proprietate Intelectuală – articole şi resurse.

http://www.dodccrp.org/iwilindex.htm

Război informaţional şi legi internaţionale, L.T. Greenberg, S.E. Goodman, K.J. Soo Hoo, NDU.

http://www.cs.georgetown.edu/~denning/infosec/ DOD-IO- legal.doc

Publicaţie amplă despre aspectele legale internaţionale ale războiului informaţional (Denning şi Baugh, 1999).

http://www.leglnet.com/libr-inwa.htm Biblioteca de legi pentru război informaţional.

Siguranţa informaţională http://www.cesg.gov.uk

Grupul pentru Securitate Comunicaţii – Electronică din UK.

http://www.itd.nrl.navv.mil/ITD/5540/main.html

Centrul Naval al SUA pentru Siguranţa înaltă a Sistemelor de

Calcul – R&D

http://cve.mitre.org

Baza de date de vulnerabilităţi şi expuneri uzuale, MITRE

http://www.robertgraham.com/pubs/network-intrusion- detection.html întrebări puse frecvent referitoare la sistemele de detecţie a intruziunii pe reţele.

http://w w w-rnks. infomatik. tu-cottbus.de/~sobirev/ids.html Rezumat şi legături la peste 80 de sisteme de detecţie a intruziunii http://www.clark.net/pub/roesch/public html/secinfo.html Lucrări şi unelte de detecţie a intruziunii, Martin Roesch.

http://jedefcnse.com

Jurnal de apărare electronică, articole orientate de Război Electronic.

http://niap.nist.gov/index.html

Parteneriatul de Siguranţă Informaţională Naţională a SUA (NIST şi NSA).

Infrastructura http://www.aph.gov.au/library/pubs/rp/1997-98/rp18.htm http://coombs.anu.edu.au/~acobb/ X0016 Australias Vulnerabi.html http://www.infowar.com/CIVIL DE/civil 100497a.html-ssi Gândind la negândit: Vulnerabilităţi australiene la atacurile informaţionale, Dr. Adam Cobb.

http://www.aracnet.com/~gtr/archive/index.html

Biografia lui Kent Anderson despre războiul informaţional şi documente de vulnerabilitate a infrastructurilor.

http://www.jwar.org

CIWARS: Jurnal de război infrastructural. http://www.nipc.gov

NIPC: Centrul de Protecţie a Infrastructurii Naţionale a SUA. http://www.pccip.gov

PCCIP: Comitetul Presidenţial al SUA pentru Protecţia Infrastructurilor Critice – PDD 63 şi raportul PCCIP.

Securitatea informaţiei http://www.cs.purdue.edu/coast/hotlist/

Arhiva CO AST la Universitatea Purdue este probabil arhiva cea mai completă de legături referitoare la securitate de pe Internet.

http://www.tno.nl/fel/infosec

URL-ografie de securitate informaţională menţinută de TNO-FEL, un punct de start pentru multe resurse referitoare la securitatea informaţiei.

Hacking http://www.attrition.org/mirTor/attrition

Site oglindă ce conţine o arhivă la zi a site-urilor web stricate, paginilor lor stricate şi a originalului lor.

http://www.ccc.de

CCC: Ggrupul de hackeri germani „Clubul de haos al calculatoarelor”

http://www.1Opht.com

Rezunat LOPHT de hacking, unelte şi articole. http://www.tno.nl/instit/fel/infosec

Resurse URL de hacking şi intimidare menţinute de TNO-FEL.

Răspuns la incidente şi urgenţe calculator http://www.cert.org

Centrul de coordonare CERT: Îndrumar de tratare a unui incident, rapoarte incident şi recomandări.

http://ciac.llnl.gov/

CIAC: Departamentul Energiei al SUA, Capabilităţi de Recomandare pentru Incidente Calculator, buletine de

securitate actualizate, unelte de securitate, informaţii despre anomalii şi alte resurse de informaţii.

http://www.assist.mil/

DOD-CERT: Departamentul Apărării SUA, anunţuri şi resurse informaţionale ale echipei de răspuns la urgenţe calculator.

http://www.first.org

FIRST: Forum de răspuns la incidente şi echipe de securitate http://www. telstra.com. au/info/securitv. html

TELSTRA: Index de referinţă australian pentru securitatea calculatoarelor şi reţelelor.

DICŢIONAR

A

ACOPERIRE acţiune militară prin care se face siguranţa trupelor ce trec de la starea de pace la cea de război, se concentrează, realizează, dispozitive de luptă sau operative, ori se retrag.

ACOPERIREA operaţia executată în perioada iniţială a războiului, de FRONTIEREI DE către grupări de forţe trecute în grabă la apărare pe STAT frontiera de stat, cu scopul de a interzice o agresiune externă, a asigura desfăşurarea oportună a mobilizării şi realizarea dispozitivului strategic de apărare.

ACOPERIREA ansamblul de acţiuni militare realizate înainte, conco- STRATEGICĂ mitent sau după declanşarea agresiunii cu rol de siguranţă strategică, desfăşurate simultan sau succesiv de către marile unităţi ale tuturor categoriilor de forţe ale armatei şi celelalte forţe ale S.N.Ap. pe frontiera de stat şi în adâncimea teritoriului, cu forţe gata de luptă permanent, pe baza unei concepţii unitare, în scopul evitării surprinderii, opririi şi respingerii agresiunii inamicului; în unele cazuri, pentru lichidarea capetelor de pod create de acesta la frontieră ori în adâncimea teritoriului naţional, asigurând condiţii favorabile executării, mobilizării şi desfăşurării tuturor forţelor participante la război.

ACŢIUNEA DE acţiunea desfăşurată de forţele armate aflate în conflinct, LUPTĂ folosind armament şi

tehnică adecvate, cu scopul de a nimici, captura sau respinge acţiunile inamicului. Se desfăşoară în mod organizat, folosindu-se forţe şi mijloace de valoare variabilă şi exprimă cel mai fidel trăsăturile caracteristice ale confruntării armate.

ACŢIUNE O anume capcacitate a Forţelor Terestre de a-şi adapta

FLEXIBILĂ misiunile şi modul de îndeplinire a acestora la o diversitate de scenarii de agresiune. Totodată acest principiu presupune o anumită abilitate în folosirea fiecărei arme (specialităţi), grupate pe module acţionale, specifice misiunii şi din perspectiva scopurilor planificate.

ACŢIUNE ansamblul măsurilor şi activităţilor concepute, planificate

MILITARĂ desfăşurate de structurile militare pentru îndeplinirea misiunilor încredinţate, concretizate în formă de luptă armată, acţiuni nonviolente sau alte forme asociate acestora.

ACŢIUNE acea acţiune prin care structurile militare sunt pregătite

MILITARĂ sau aduse în starea din care să poată desfăşura acţiuni

ASOCIATĂ militare de luptă sau nonviolente.

ACŢIUNE acea acţiune prin care o structură militară îşi pune în

MILITARĂ aplicare forţa, de regulă, fără întrebuinţarea arma-NONVIOLENTĂ mentului.

ACŢIUNEA exprimă necesitatea de a dispune marile unităţi şi unităţile

RAPIDĂ constituite în structuri mobile cu mare putere de foc şi cu independenţă logistică, capabile de a riposta ferm şi decisiv, în orice zonă (punct) de interes strategic.

ACŢIUNILE reprezintă un model de operaţionalizare a zonei de

INTEGRATE operaţii şi a teatrului de acţiuni militare de interes strategic, având ca notă dominantă acţiunea comună a tuturor/a majorităţii forţelor participante la

acţiuni militare, în vederea atingerii unui scop comun.

ACŢIUNI formă de acţiune dusă cu mijloace ilegale, contrare

SUBVERSIVE normelor democratice specifice ordinii de drept, care vizează destabilizarea sistemului politic, dezorganizarea statului şi a societăţii pentru a li se putea impune mai uşor condiţiile care le lezează securitatea. Reprezintă o combinare a mijloacelor şi metodelor teroriste cu cele proprii luptei politice, economice, psihologice sau de altă natură.

ACŢIUNI agresiuni interne ilegale, imprevizibile, oculte, extrem

TERORISTE SI de violente, ce se execută asupra unor obiective TERORIST- aparţinând forţelor operaţionale din raioanele acţiunilor

DIVERSIONISTE de luptă, precum şi asupra unor obiective politice, strategice, teritoriale, demografice, etnice, diplomatice din zona interioară a ţării.

ADAPTABILITATE capacitatea sistemului militar de a răspunde cu promptitudine la modificările apărute în înzestrare, organizare, concepte, proceduri şi misiuni, fără diminuarea caracterului planificat şi organizat.

ADÂNCIME dimensiune spaţială, măsurată de la linia frontului spre spatele acestuia, în limitele căruia sunt realizare dispozitivele subunităţilor, unităţilor şi marilor unităţi destinate să îndeplinească o misiune de luptă atât în ofensivă cât şi în apărare.

ADÂNCIMEA adâncimea spaţială din dispozitivul inamicului ce

MISIUNII urmează să fie cucerită şi care se stabileşte prin conţinutul misiuniii. Se măsoară de la limita dinainte a apărării inamicului şi până la un aliniament situat în interiorul sau înapoia obiectivului ce urmează să fie cucerit.

AGILITATE uşurinţă în mişcări; supleţe, sprinteneală, vioiciune.

AGRESIUNE atac împotriva unei persoane sau a unui stat.

AGRESIUNE folosirea forţei armate de către un stat împotriva

ARMATĂ suveranităţii, integrităţii teritoriale sau independenţei politice a unui stat în orice mod incompatibil cu Carta Naţiunilor Unite.

ALIANŢĂ^ înţelegere înscrisa într-un tratat prin care statele semnatare

MILITÂRĂ îşi asumă obligaţia reciprocă de a acţiona cu toate sau numai cu o parte din forţele lor armate împotriva unui adversar comun.

AMENAJAREA totalitatea lucrărilor genistice de fortificaţie, baraje,

GENISTICĂ distrugeri, drumuri, poduri, treceri, mascare, asigurare cu apă şi de adaptare a localităţilor, zonelor puternic industrializate, obiectivelor economice importante, obstacolelor şi acoperirilor terenului din fâşia (zona) de acţiune a marii unităţi strategice (operative, tactice), executate într-o concepţie unitară, în scopul interzicerii, îngreunării sau reducerii efectelor acţiunilor inamicului (adversarului) şi asigurării condiţiilor favorabile acţiunilor trupelor proprii.

AMENINŢARE săvârşirea de către un stat sau mai multe state a unor acte

CU FORŢA politice, economice, militare sau de altă natură, cu scopul de a impune altui stat să renunţe la deplina exercitare a drepturilor şi atributelor suverane. Este o acţiune contrară principiilor şi normelor de raporturi între state.

ANGAJARE 1. situaţie în care trupele se găsesc în contact cu inamicul şi desfăşoară acţiuni de luptă; 2. introducerea în luptă a unor forţe.

APĂRAREA forma de luptă armată prin care se realizează respingerea, oprirea sau întârzierea acţiunilor inamicului, în scopul menţinerii spaţiului (terestru, aerian, maritim, fluvial) sau obiectivului încredinţat.

APĂRAREA capcacitatea sistemului defensiv de a lovi inamicul, în

ACTIVĂ toate situaţiile, prin foc la distanţă mare,

prin riposte ofensive violente sau prin procedee de acţiune ofensive, dirijate asupra părţilor vulnerabile ale dispozitivului advers.

APĂRAREA ansamblul măsurilor şi acţiunilor militare desfăşurate

ARMATĂ A unitar de Sistemul Naţional de Apărare în spaţiul terestru,

ŢĂRII aerian şi maritim (fluvial) în scopul descurajării, zădărnicirii şi respingerii oricărei acţiuni militare care ar leza interesele fundamentale ale ROMÂNIEI.

APĂRAREA adaptabilitatea promptă a Sistemului Naţional de Apărare

FLEXIBILĂ la orice context întrevăzut în prognoza strategică precum şi asigurarea posibilităţilor de a îmbina acţiunile de menţinere fermă a celor mai importante raioane, obiective şi aliniamente cu riposte ofensive ce vizează scopuri decisive.

APĂRAREA ÎN procedeul prin care forţele menţin o suprafaţă de teren ÎNCERCUIRE (zonă, obiectiv), luptând cu un inamic care este dispus în jurul lor şi acţionează pe toate direcţiile.

APĂRAREA formă de ducere a luptei care se bazează pe folosirea unor

MOBILĂ acţiuni combinate, ofensive şi de apărare, întârzietoare, în scopul canalizării acţiunilor inamicului pe o direcţie care să ofere apărătorului condiţii avantajoase pentru executarea ripostelor ofensive în flancuri şi spatele inamicului, şi care, în final, să ducă la încercuirea şi nimicirea grupării principale de forţe, la refacerea dispozitivului pe aliniamentul iniţial, iar pe direcţiile pe care înainteaza cu succes, chiar la generalizarea atitudinii ofensive.

APĂRAREA^ totalitatea măsurilor şi acţiunilor adoptate şi desfăşurate NAŢIONALĂ de autorităţile constituţionale ale statului român în scopul garantării suveranităţii naţionale, independenţei şi unităţii statului, integrităţii teritoriale a ţării şi a democraţiei

constituţionale.

APĂRAREA ansamblul de măsuri şi acţiuni ce se desfăşoară în scopul

N.B.C. menţinerii capcacităţii de luptă a trupelor în condiţiile contaminării radioactive, biologice şi chimice. Aceasta se realizează prin: evaluarea posibilităţilor şi cunoaşterea intenţiilor inamicului privind întrebuinţarea armelor de nimicire în masă; determinarea efectelor şi urmărilor în cazul folosirii acestora; stabilirea măsurilor de protecţie specifice şi executarea decontaminării trupelor şi terenului.

APARAREA procedeu defensiv care permite forţelor angajate în luptă

PREGĂTITĂ DIN să-şi pună în aplicare, în volum complet elementele TIMP puterii de luptă.

APĂRAREA ä procedeu defensiv care permite forţelor angajate în luptă PREGĂTITĂ ÎN să-şi pună în aplicare, în volum redus, elementele puterii GRABĂ de iuptă.

APĂRAREA formă particulară a operaţiei de apărare ce se adoptă în

ZONALĂ plan local, în care forţele dintr-o anumită zonă acţionează întrunit, după o concepţie unitară, pentru respingerea ofensivei inamicului şi nimicirea acestuia.

ARTA componentă a ştiinţei militare care are ca obiect de studiu

MILITARĂ teoria şi practica organizării şi ducerii luptei armate, a războiului în ansamblu. Studiază experienţa luptei armate, elaborând principii, reguli, norme, procedee şi metode de pregătire şi ducere a acţiunilor militare în timp de război.

ASIGURAREA ansamblul de măsuri şi acţiuni, desfăşurare continuu într- ACŢIUNILOR ŞI o concepţie unitară, de către toate forţele participante şi PROTECŢIA la toate eşaloanele, destinate obţinerii datelor necesare şi

TRUPELOR creării condiţiilor de securitate a personalului, tehnicii şi sistemelor împotriva acţiuniii agresorului şi a altor factori perturbatori, executate în scopul menţinerii capacităţii de luptă a trupelor şi

îndeplinirii misiunilor primite.

ASIGURAREA ansamblul de măsuri şi acţiuni ce se întreprind pentru: CĂILOR DE alegerea, recunoaşterea şi pregătirea căilor de

COMUNICAŢIE comunicaţii; repararea, restabilirea, întreţinerea, paza şi menţinerea în stare de viabilitate a dumurilor, căilor ferate, gărilor, porturilor, aeroporturilor şi lucrărilor de artă; organizarea şi executarea serviciului de comenduire şi îndrumare a circulaţiei; cercetarea nucleară, biologică şi chimică pe căile de comunicaţii, paza şi apărarea lucrărilor de artă de pe acestea.

ASIGURAREA totalitatea măsurilor ce se iau în scopul stabilirii, cererii, FINANCIARĂ obţinerii, utilizării şi justificării mijloacelor financiare destinate forţelor armate, pentru a le aproviziona la timp şi fără întrerupere cu tehnică şi materiale, precum şi pentru plata drepturilor băneşti cuvenite personalului.

ASIGURAREA totalitatea măsurilor ce se iau în vederea păstrării sănătăţii MEDICALĂ militarilor, prevenirii apariţiei şi răspândirii bolilor, acordării la timp a ajutorului medical, evacuării răniţilor şi bolnavilor şi spitalizării, tratamentului şi recuperării acestora în scopul înapoierii în cel mai scurt timp la unităţi.

ASIGURAREA menţinerea sănătăţii a animalelor şi prevenirea SANITAR- transmiterii bolilor de la animale la om, tratarea şi

VETERINARA evacuarea animalelor rănite şi bolnave, cunoaşterea stării epizootice din zonă, controlul sanitar-veterinar al alimentelor de origine animală, protecţia sanitarveterinară împotriva efectelor armelor de nimicire în masă, aprovizionarea forţelor cu animale pentru serviciu.

ASIGURAREA ansamblul de măsuri, activităţi şi operaţiuni care se TEHNICĂ planifică, organizează şi execută în scopul menţinerii în permanenţă a unui înalt grad de completare cu tehnică militară şi unei stări tehnice şi de întreţinere bună a acesteia, precum şi a evacuării tehnicii deteriorate de pe câmpul de luptă.

ASISTENTĂ totalitatea măsurilor şi acţiunilor întreprinse pentru a se

JURIDICĂ asigura respectarea în acţiunile militare a cerinţelor legilor ţării, regulamentelor militare şi ale dreptului internaţional aplicabil în conflictele armate.

ASISTENTĂ înţelegere politico-militară între două sau mai multe state

MUTUALĂ pentru apărarea comună împotriva unui atac armat.

ASISTENŢĂ^ asistenţa militară sau civilă acordată de o forţă străină NAŢIONALĂ unei naţiuni prin intervenţia pe teritoriul ţării resprective, pe timp de pace, în situaţii de criză sau război, în baza unor acorduri încheiate pe bază de reciprocitate.

ASISTENTĂ acţiuni desfăsurate pentru înlăturarea efectelor dezastrelor

UMANITĂRĂ naturale sau provocate de om, fiind limitate ca sop şi durată, ele suplimentând sau completând eforturile depuse de naţiunea în cauză.

ATITUDINE anticiparea posibilelor ameninţări şi a situaţiilor de risc;

MENTALĂ „ w vizează singerea „din faşă" a unor focare de conflict, a PREVENTIVĂ" căror extindere, scăpând de sub control, ar putea aduce atingerea intereselor naţionale ale României.

ATITUDINE orientarea spre înfrângerea ulterioară a unui inamic

MENTALĂ „ evident şi cunoscut în toate componentele sale. REACTIVĂ"

ATRIBUT (AL o activitate, o obligaţie de a îndeplinii anumite sarcini CONDUCERII) sau operaţii ce se pot încredinţa unui organ de conducere, compartiment sau persoană şi care este dimensionat de structura sistemului şi factorii care îl influenţează.

AUTORITATE dreptul de a da ordine pe care un militar şi-l asumă potrivit ASUMATĂ actelor normative în vigoare, a ierarhizării gradelor,

LEGAL funcţiilor şi a competenţelor în domeniu.

B

confruntare cu rol decisiv, din cadrul operaţiei, prin care

BĂTĂLIE se asigură obţinerea succesului în îndeplinirea obiectivului (scopului) urmărit de aceasta.

BLOCADĂ acţiune desfăşurată de forţe externe pentru întreruperea căilor de legătură maritime, terestre, aeriane, fluviale, a fluxurilor vitale de surse energetice, materii prime şi materiale strategice, necesare desfăşurării normale a activităţilor obiectivelor economice de importanţă vitală etc.

C

CALITATE totalitatea însuşirilor şi laturilor esenţiale în virtutea cărora un lucru este ceea ce este, deosebindu-se de celelalte lucruri.

CAMPANIA totalitatea operaţiilor şi luptelor forţelor armate desfăşurate într-o perioadă de timp caracteristică (an, anotimp) sau într-o zonă geografică distinctă, pe baza unei concepţii unitare, în vederea îndepliniii unor obiective strategice.

CAPABILITATE posibilitatea de a săvârşi ceva, de a fi în stare să execute ceva.

CAPACITATE ansamblul cunoştinţelor, abilităţilor, însuşirilor psihice şi comportamentelor necesare agentului acţiunii militare pentru realizarea unor acţiuni determinate.

CAPACITATEA capacitatea de reacţie a armatei în situaţiile care necesită

ACTIONALĂ A interventia sa.

STRUCTURILOR

CAPACITATE principiul de bază al organizării Forţelor Terestre în timp

DEFENSIVĂ de pace, care presupune restructurarea acestora în scopul

CREDIBILĂ realizării unei structuri militare descurajante, active, mobile, robuste, flexibile şi suficiente, capabilă să asigure opreaţionalizarea unei forţe de reacţie ample şi eficiente.

CAPACITATE posibilitatea unităţii de a desfăşura acţiuni militare în

OPERAŢIONALĂ conformitate cu scopul pentru care a fost creată.

CAPACITĂTI posibilităţile unei unităţi de a desfăşura pe lângă spfctat f ' acţiunile de bază pentru care a fost creată şi acţiuni complementare (nucleare, biologice şi chimice; război electronic; apărare antiaeriană; apărare antiblindate; supraveghere electronică etc.).

CARACTERUL asigură instruirea comandamentelor şi trupelor în INTERARME ŞI condiţiile reale şi complexe ale câmpului modern de luptă INTEROGATORII când misiunile nu mai pot fi îndeplinite decât cu DE FORŢE participarea în funcţie de amploarea forţelor angajate, a tuturor armelor şi categoriilor de forţe aflate la dispoziţia eşalonului tactic, operativ sau strategic.

CARACTERUL presupune desfăşurarea acţiunilor militare într-un ritm PULSATORIU viu, trepidant în spaţiul de confruntare. (AL CÂMPULUI DE LUPTĂ)

CARACTER spaţiul de confruntare poate fi terestru, aerian şi maritim

TRIDIMENSIONAL (fluvial). (AL CÂMPULUI DE LUPTĂ)

CAZAREA totalitatea măsurilor şi acţiuftilor ce se execută în scopul:

TRUPELOR SI asigurării cu terenuri, constructii, instalaţii şi ADĂPOSTIREA aprovizionarea cu materiale specifice; exploatării, ANIM ALELOR întreţinerii şi reparării construcţiilor şi instalaţiilor; cazării personalului şi adăpostirii animalelor în clădiri, corturi, adăposturi, vehicule speciale etc.; prevenirii şi stingerii incendiilor.

CÂMP DE spaţiul în care se desfăşoară acţiunile militare în

LUPTĂ confruntarea directă şi nemijlocită dintre părţile beligerante.

CAMP DE spaţiul de confruntare definit prin următoarele elemente:

LUPTĂ multitudinea sistemelor automatizate de

armament şi

CIBERNETIZAT roboţi utilizaţi pe câmpul de luptă; condiţii impuse de comprimarea timpului operativ; multifuncţionalitatea forţelor luptătoare; conservarea forţelor umane prin folosirea lor masivă numai în situaţii de mare dinamism; compensarea limitelor fiziologice ale comandanţilor, luptătorilor şi operatorilor prin utilizarea roboţilor pentru activităţi care cer eforturi şi timp îndelungat, atenţie deosebită, migală, precizie, sacrificiu etc.

CÂMP DE spaţiul terestru, aerian şi – după cazmaritim sau fluvial

LUPTĂ în care se dispun şi duc lupte integrate forţele şi mijloacele

INTEGRAT marilor unităţi şi unităţilor tactice de arme întrunite, şi cele aparţinând celorlalte categorii de forţe armate care sunt subordonate temporar sau cu care cooperează, în vederea îndeplinirii misiunilor.

CERCETARE w disciplină ştiinţifică ce cuprinde un ansamblu de principii, OPERAŢIONALĂ metode şi mijloace destinate elaborării de metodele matematice ale fenomenelor şi proceselor studiate. Are ca obiectiv fundamnetarea cantitativă a hotărârilor, prin elaborarea variantelor şi criteriilor decizionale, studiul consecinţelor imediate şi de perspectivă ale acestora, evaluarea diferiţilor factori de influenţă.

CIOCNIREA angajarea inamicului de către forţele proprii în confruntarea militară. Se desfăşoară în timp scurt şi, de regulă, este dusă de eşalonul brigadă (similar) şi de inferioarele acestuia. Are loc, de regulă, între elementele de siguranţă ale forţelor adverse şi se poate transforma sau nu în luptă.

COEZIUNEA coeziunea este unitate. Aceasta este o calitate care leagă împreuna părţile componente, care furnizează rezistenţă (elasticitate) împotriva acţiunilor distructive şi a dezorganizării. Micşorează vulnerabilitatea structurilor la înfrângere şi împotriva efectelor loviturilor adverse.

COLABORARE promovarea şi apărearea intereselor naţionale în relaţiile MILITARĂ w cu partenerii de dialog pentru edificarea unei arhitecturi INlfcKNAŢIONALĂ de securitate viabile, care să contribuie la întarirea încrederii şi a transparenţei relaţiilor dintre Armata României şi armatele altor ţări.

COMANDA ansamblul acţiunilor prin care organul de conducere îşi impune voinţa asupra organelor de execuţie pentru a acţiona în sensul dorit; a comanda semnifică punerea în aplicare a unor decizii, planuri sau programe concepute în prealabil în vederea realizării obiectivului/scopului propus.

COMANDAMENTUL este format din personal provenit din armatele a două COMBINAT sau mai multe ţări.

OQMANDAMENTUL structură de comandă, de concepţie şi execuţie ce FORŢELOR răspunde de întrebuinţarea forţelor şi mijloacelor din

TERESTRE subordine; se înfiinţeaza la război şi se subordonează ierarhic Marelui Cartier General.

OOMANDAMENIUL este f°rmat din personal provenit din două sau mai multe ÎNTRUNIT categorii de forţe ale armatei şi are în principiu structura unui comandament obişnuit.

rnMANDAMFNTliï structura de comandă, de concepţie şi execuţie ce TnrrsTTr AT răspunde de organizarea, planificarea şi întrebuinţarea FnPTn np forţelor şi mijloacelor de logistică din subordine;

TCDCCTDC funcţionează la pace, în situaţii de criză şi război şi se

TERESTRE subordonează ierarhic Statului Major al Forţelor Terestre

(Comandamentului Forţelor Terestre).

COMANDAMENTUL organism ce trebuie să aibă o structură care să permită OPERAŢIONAL planificarea operaţiilor integrate, dar şi conducerea şi INTER ARME controlul specific al forţelor din subordine.

COMANDAMEVIUL structura de comandă ce are în

subordine nemijlocită OPERAŢIONAL forţele operaţionale de nivel operativ/tactic. OPERATIV/ TACTIC

COMBATEREA totalitatea acţiunilor care includ antiterorismul (măsuri TERORISMULUI defensive luate pentru reducerea vulnerabilităţii în faţa actelor de terorism) şi contraterorismul (măsuri luate pentru a împiedica, intimida şi reacţiona la actele de terorism) desfăşurate în scopul combaterii terorismului în toată gama ameninţărilor pe care le implică.

COMPATIBILI- capacitate a două sau mai multe părţi de a funcţiona TĂTE împreuna fără o interferenţă reciprocă.

COMPETENŢĂ normă strategică a organizării şi executării instrucţiei şi educaţiei militare, semnificând totalitatea capacităţilor cognitive, psihomorale şi psihomotrice prin care agentul acţiunii militare acţionează individual şi/sau în grup, pentru a asigura fucţionalitatea structurii militare din care face parte.

COMPETENŢĂ ^ selecţionarea celor mai competente cadre şi încadrarea PROFESIONĂLĂ acestora pe funcţiile prevăzute în structurile care (A MANAGE- planifică, organizează şi coordonează instrucţia armatei. MENTULUI INSTRUCŢIEI)

COMFEimVITAIE dorinţa fiecărui militar de a fi cel mai bun şi de a se compara permanent cu ceilalţi „în spiritul concurenţei.

COMPLEMENTA- transferul cunoştinţelor şi formarea deprinderilor necesare RIT ATE „luptătorului universal” carc poate folosi în mod real toate categoriile de armament individual şi tehnica de luptă din înzestrarea subunităţii.

COOPERAREA activitatea prin care se asigură coordonarea acţiunilor tuturor forţelor participante la luptă (operaţie) în timp, spaţiu şi pe misiuni, în scopul concentrării şi însumării eforturilor acestora pentru îndeplinirea unei misiuni de luptă comune.

COORDONAREA activitatea de menţinere, păstrare şi perfecţionare a stării de ordonare a sistemului conducător

şi a celui condus, precum şi a tuturor relaţiilor dintre ele.

COORDONAREA ansamblul proceselor prin care se sincronizează deciziile INSTRUCŢIEI şi acţiunile personalului sistemului de instrucţie al armatei, în ceea ce priveşte dirijarea resurselor, astfel încât, acestea să fie disponibile la timpul necesar, în cantitatea şi de calitatea stabilită, în scopul realizării obiectivelor propuse.

COORDONAREA sincronizarea acţiunilor structurilor care planifică şi

INSTRUCŢIEI conduc procesul de instrucţie în vederea realizării

ARMATEI obiectivelor stabilite. (FUNCŢIE)

CONDUCEREA mulţimea acţiunilor întreprinse de manager în vederea

INSTRUCŢIEI aplicării deciziilor prin exercitarea atribuţiilor de comandă şi control.

CONDUCEREA ca activitate, este un atribut al Comandamentului Forţelor FORŢELOR Terestre, iar ca element component al sistemului de

TERESTRE conducere al sistemului de conducere al armatei, este construit din structuri de comandă cu atribuţii şi responsabilităţi în conceperea, administrarea şi armonizarea măsurilor şi acţiunilor destinate apărării, pentru trupele din subordine.

CONDUCEREA ^ totalitatea activităţilor şi măsurilor întreprinse de către OPERAŢIONALA organele de conducere în scopul organizării şi desfăşurării luptei armate.

CONTINUĂRI moduri probabile de acţiune bazate pe rezultatele posibile ale secvenţelor sau ale cursului unei acţiuni militare.

CONTINUITATE faptul, însuşirea de a fi continuu, starea a ce este continuu.

CONFLICT confruntarea între două sau mai multe state, folosind forţa

ARMAT armată, care urmăreşte rezolvarea unor neînţelegeri sau diferende de interese, atunci când reglementarea paşnică nu a reuşit să le rezolve.

CONTRALOVI- ripostă ofensivă desfăşurată în spaţiul operativ de către TURĂ mari unităţi, cu scopul de a nimici gruparea principală de forţe a inamicului pătruns în fâşia de apărare a unei mari unităţi operative.

CONTRAPRE- acţiunea de lovire prin foc masat, executată prin GĂTIREA surprindere, cu toate mijloacele la dispoziţie, asupra obiectivelor şi grupărilor principale de forţe ale agresorului pregătite pentru ofensivă.

CONTROLUL activitatea de cunoaştere a relaţiilor şi a modului de aplicare a actelor normative ce reglementează activitatea domeniului militar.

CONTROLUL implică orice plan, aranjament sau proces bazat pe

ARMAMENTELOR acorduri internaţionale şi guvernează oricare dintre aspectele privind numărul, tipurile şi caracteristicile performanţelor sistemelor de armamente, forţa numerică, organizarea, echiparea şi dislocarea forţelor armate menţinute de părţi în scopul reducerii instabilităţii în mediul militar.

CONTROLUL ansamblul activităţilor desfăşurate de structurile

SISTEMULUI DE sistemului în vederea verificării stadiului de pregătire la

INSTRUCŢIE un moment dat în comparaţie cu oviectivele stabilite pentru s dr interveni a se elimina neajunsurile care împiedică realizarea programului de instrucţie.

CORPUL DE mare unitate operativă, destinată să îndeplinească misiuni

ARMATA de apărare zonală, mobilizare şi instruire a rezerviştilor.

TERITORIAL Are în compunere mari unităţi (unităţi, subunităţi) de arme întrunite, de armă şi de asigurare a acţiunilor de luptă.

CREDIBILITATE capacitatea organismului militar de a induce pe plan intern şi extern percepţii şi convingeri ferme cu privire la potenţialul de care dispune, pentru a desfăşura cu succes acţiuni armate.

CRIZĂ manifestare a unor dificultăţi (economice, politice, sociale etc.); perioadă de tensiune, de tulburare, de încercări (adesea decisive) care se manifestă în societate. Moment critic care intervine în evoluţia vieţii internaţionale, a raporturilor dintre state, a unui sistem, regim sau guvern.

D

DEBARCARE moment (etapă, fază) din acţiunea de desantare care cuprinde atingerea solului de către desantul aerian paraşutat sau aerotransportat şi lupta pentru ocuparea primelor raioane ale subunităţilor desantate.

DECIZIE hotărâre luată în urma examinării unei probleme, a unei situaţii etc., soluţie adoptată (dintre mai multe posibile); rezoluţie.

DEGREVARE acţiunea de a degreva (a scădea, a reduce sarcinile sau obligaţiile impuse unei persoane fizice sau unei instituţii) şi rezultatul ei.

DEMONSTRAŢIE operaţiune menită să demonstreze capacitatea militară a

DE FORŢĂ unei alianţe, a unui stat sau a unei grupări de trupe dislocate într-o anumită zonă, în încercarea de a dezamorsa o anumită situaţie.

DEPLASAREA acţiunea prin care marile unităţi (unităţile şi subunităţile) şi grupările de forţe sunt dislocate dintr-un loc în altul.

DEPLASAREA acţiunea prin care o structură militară se deplasează prin

COMBINATĂ marş şi prin transport.

DEPLASAREA acţiune desfăşurată de trupe pentru mutarea dintr-un raion

TRUPELOR în altul, intrarea în luptă sau efectuarea unei manevre, cu păstrarea completă a capacităţii de luptă în vederea îndeplinirii unei misiuni.

DESANT grupe de forţe făcând parte din dispozitivul de luptă

AERIAN (operativ sau strategic), transportată pe calea aerului (cu avioane, elicoptere, planoare) şi

întrebuinţată, de regulă, în raioane din adâncimea dispozitivului inamicului, prin debarcare sau paraşutare în scopul îndeplinirii unei misiuni de luptă. Forţele utilizate pot fi trupe de paraşutişti sau trupe de orice armă, antrenate pentru ducerea unor astfel de acţiuni.

DESCOPERIRE acţiunea de a descoperi (a găsi un lucru căutat, necunoscut sau ascuns; a afla) şi rezultaul ei; ceea ce a fost descoperit, aflat.

DESCURAJARE concept al unor doctrine militare contemporane, potrivit căruia se urmăreşte a determina adversarul să renunţe la anumite scopuri, acţiuni, mijloace, de teama ripostei şi a riscurilor pe care le-ar atrage folosirea acestora.

DESCURAJARE constituirea şi dezvolatarea permanentă a unor forţe

ACTIVĂ convenţionale care să reprezinte un factor descurajant potrivit pentru un potenţial adversar.

DESCURAJATOR care te face să-ţi peirzi curajul; demoralizant; deprimant.

DESFĂŞURARE ansamblul de măsuri organizatorice şi de planificare,

STRATEGICĂ precum şi activităţile practice începute încă din timp de pace şi continuate în perioada de tensiune în relaţiile internaţionale sau după declanşarea acţiunilor militare, pentru trecerea forţelor armate şi a forţelor de protecţie de la starea de pace la cea de război, rirdicându-le capacitatea de luptă în trepte (succesiv) sau direct prin mobilizare, deplasarea lor în siguranţă, către frontiera de stat, crearea grupărilor de forţe şi a dispozitivului strategic de apărare preconizat, concomitent cu trecerea economiei naţionale la producţia de război.

DETENSIONARE acţiunea de a detensiona (a elimina sau a reduce tensiunea) şi rezultatul ei.

DEVANSARE o acţiune de depăşire a inamicului, în timp şi spaţiu, cu scopul de a-l surprinde şi de a-i micşora şansele, de a opune rezistenţă organizată. Se realizează exploatând rapid condiţiile favorabile manifestate într-un moment.

DEZORGANI- acţiune prin care se urmăreşte perturbarea gravă a

ZARE sitemului de conducere a trupelor inamicului şi a comunicaţiilor acestuia.

DIFEREND deosebiri de păreri între două sau mai multe persoane, state etc.; neînţelegere, dezacord.

DIGITAL care generează, măsoară, prelucrează, sau stochează semnale digitale.

DIGITALIZARE acţiunea de transformare a semnalelor analogige în semnale digitale.

DIGITALIZAT care a fost transformat în semnal digital.

DINAMIC plin de mişcare, de acţiune, activ; care este în continuă

(şi intensă) mişcare, evoluţie, care se desfăşoară rapid.

DINAMISM putere vitală, forţă de acţiune, de mişcare.

DIPLOMAŢIE acţiuni diplomatice întreprinse înaintea unei crize

PREVENTIVĂ previzibile, pentru prevenirea şi limitarea violenţelor.

DISCONTINUI- lipsă de continuitate între mai multe elemente care se

TĂTE succed în timp sau în spaţiu; intermitenţă.

DISPOZITIV DE dispozitiv constituit în vederea desfăşurării acţiunilor de

LUPTĂ luptă, care materializează hotărârea comandantului privind modalitatea de întrebuinţare a forţelor şi mijloacelor pentru îndeplinirea misiunii.

DISPUNEREA impune (în dimensiunea ei operativă şi tactică)

AVANSATĂ A „prepoziţionarea” unor forţe pe direcţiile strategice,

FORŢELOR operative şi chiar tactice, care să constituie un nucleu

(cu o prezenţă înaintată) mobil cu rolul de a prelua „şocul” primelor acţiuni militare desfaşurate în forţă.

DIVERSIUNE 1. acţiune desfăşurată cu scopul de a-l induce în eroare pe inamic asupra direcţiei principale de atac (direcţii/ lovituri principale) sau a zonei (raionului) în care se pregătesc anumite acţiuni de luptă. 2. acţiune executată de grupări specializate pe teritoriul părţii adverse cu scopul de a slăbi capacitatea de rezistenţă şi moralul populaţiei şi al militarilor, folosind procedee specifice (sabotaje, răspândirea de zvonuri, manifeste etc.).

DOCTRINĂ totalitatea principiilor unui sistem politic, ştiinţific, religios, militar.

DOCTRINA DE ansamblul tezelor, principiilor, regulilor şi normelor INSTRUCŢIE A adoptate de organismul militar cu privire la instrucţia ARMATEI Armatei României, astfel încât aceasta să-şi poată îndeplini misiunile ce-i revin pe timp de pace, în situaţii de criză şi la război, potrivit prevederilor Constituţiei României şi legilor în vigoare.

DOCTRINA concepţie unitară adoptată de stat cu privire la război,

MILITARĂ armată şi apărarea ţării, ansamblul principiilor, metodelor şi procedeelor preconizate şi aplicate în pregătirea forţelor armate, a populaţiei şi în ducerea războiului, în raport cu condiţiile, interesele şi posibilităţile specifice ale statului.

DOCTRINA ^ totalitatea principiilor, operaţiunilor, metodelor, OPERAŢIONALĂ obiectivelor şi direcţiilor de acţiune a Forţelor Terestre A FORŢELOR precum şi concepţia de organizare, înzestrare şi TERESTRE întrebuinţare a acestora pe timp de pace, în situaţii de criză şi la război, pentru îndeplinirea misiunilor ce le revin potrivit prevederilor legilor ţării şi ale regulamentelor militare în vigoare.

DREPT totalitatea normelor de drept care reglementează

INTERNAŢIONAL raporturile dintre state.

DREPT parte a dreptului internaţional care asigură securitatea

INTERNAŢIONAL persoanelor civile, militarilor răniţi sau bolnavilor, UMANITĂR personalului medical şi forţelor de protecţie civilă în caz de conflict armat şi a populaţiei de pe teritoriile ocupate.

DURATA timpul necesar pentru exercitarea actului de comandă din

CICLULUI momentul primirii misiunii sau informaţiilor despre

CONDUCERII modificări esenţiale ale situaţiei până când eşalonul condus este capabil să desfăşoare acţiuni în concordanţă cu decizia comandantului.

E

ECHIPA grup de oameni (militari) care, sub conducerea unui şef, îndeplinesc/execută în acelaşi timp o muncă/misiune sau o acţiune comună.

ECONOMIA DE stabilirea, distribuirea şi utilizarea judicioasă a FORŢE ŞI posibilităţilor de luptă proprii, în raport cu necesităţile

MIJLOACE impuse de obiectiv şi de obţinerea de rezultate maxime cu eforturi, forţe, mijloace şi pierderi minime.

EFICACITATE măsura în care o activitate satisface o necesitate, realizează un obiectiv, îndeplineşte o funcţie; poate fi pozitivă, nulă sau negativă.

EFICIENŢĂ raportul dintre eficacitate şi costuri.

EFICIENŢA gestionarea judicioasă a resurselor materiale şi financiare,

MANAGEMEN- puse la dispoziţie pe o perioadă delimitată de timp, astfel

TULUI încât cu resurse minime să se obţină rezultate maxime. INSTRUCTIEI ARMATEI

EFORT DE totalitatea eforturilor materiale, umane, culturale, pe care

APĂRARE un stat le face pentru apărarea proprie sau a aliaţilor în cazul unei agresiuni.

ESTIMARE activitate prin care un compartiment, în urma unui proces de analiză, emite concluzii şi propuneri (necesitate; posibilitate; mod de rezolvare; cerinţe

operaţionale, materiale, financiare) cu privire la o situaţie, misiune sau ordin.

F

FLEXIBILITATEA exprimă o caracteristică a conducerii care se răsfrânge ACŢIUNILOR asupra elasticităţii şi supleţei execuţiei şi desemnează MILITARE capacitatea comandamentelor de a prevedea evoluţiile ulterioare, precum şi de a adapta rapid atât ele cât şi trupele, la schimbările dese şi neaşteptate care au loc pe câmpul de luptă.

FLEXIBILITATEA capacitatea sistemului de instrucţie de a permite INSTRUCŢIEI extinderea/diminuarea unor activităţi, schimbarea/ MILITARE redimensionarea obiectivelor în funcţie de priorităţile impuse.

FLEXIBILITATEA adoptarea formelor optime de organizare, funcţie de

MANAGEMEN- schimbările survenite în sistemul militar NATO, în

TULUI strânsă concordanţă cu influenţele pe care le oferă

INSTRUCŢIEI resursele umane, materiale şi financiare avute la dispoziţie.

FOLOSIREA corelarea strictă a obiectivelor cu resursele avute la

EFICIENTĂ A dispoziţie astfel încât, pentru fiecare obiectiv de instrucţie

RESURSELOR să se consume numai cât este necesar.

FORŢE DE mari unităţi (unităţi) de armă şi specialităţi, dispuse pe

ANGAJARE limita dinainte a dispozitivului şi întrebuinţate pentru

IMEDIATĂ producerea de pierderi cât mai mari agresorului, slăbirea

(F.A.I.) capacităţii de luptă şi oprirea ofensivei acestuia, limitarea pătrunderii în adâncimea apărării, menţinerea zonelor (fâşiilor, raioanelor) încredinţate şi crearea condiţiilor necesare trecerii la ofensivă.

FORŢE DE acele forţe dispuse în adâncimea

dispozitivului în scopul

ANGAJARE executării ripostelor ofensive, apărării unor raioane

ULTERIOARĂ (aliniamente) din adâncime, nimicirii desantului aerian (F.A.U.) (maritim) şi trupelor aeromobile, înlocuirii unor grupări din forţele de angajare imediată care au suferit pierderi mari şi închiderii unor breşe din dispozitiv apărute ca urmare a întrebuinţării de către agresor a armelor N.B.C.

FORŢE DE forţe destinate să susţină forţele angajate pentru

SPRIJIN (F.S.) îndeplinirea scopurilor operaţiei. Ele cuprind, de regulă, mari unităţi (unităţi, subunităţi) de artilerie şi rachete, artilerie antitanc, aviaţie de sprijin, artilerie şi rachete antiaeriene, cercetare, război electronic, radiolocaţie, geniu, protecţie N.B.C., mijloace incendiare şi furnizare.

FORŢE principala categorie de forţe destinate să desfăşoare

TERESTRE (F.T.) acţiuni militare întrunite, independent sau în comun cu celelalte forţe, pentru apărarea armată a ţării, în orice zonă de operaţii, condiţii de climă şi relief şi reprezintă forţa întrunită, capabilă să realizeze prezenţa, extinderea, continuitatea şi dominaţia în teren şi să susţină în orice moment toată gama acţiunilor militare necesare îndeplinirii scopului propus. Ele au capacitatea de a se proiecta rapid, generând forţe care să răspundă cerinţelor în situaţii de criză, cât şi forţe redimensionate pentru starea de război, prin mobilizarea resurselor puse la dispoziţie.

FORŢE acele forţe destinate intervenţiei pentru gestionarea

TERESTRE DE situaţiilor de criză care pun în pericol interesele naţionale REACŢIE ÎN fundamentale, asigurării îndeplinirii angajamentelor

SITUAŢII DE militare internaţionale asumate de România, participării

CRIZĂ la prevenirea, limitarea şi înlaturarea

urmărilor unor

(F.T.R.S.C.) dezastre.

FORŢE grupare de forţe constituită din mari unităţi şi unităţi

TERESTRE DE mecanizate, de tancuri, vânători de munte, paraşutişti şi REACŢIE poliţie militară, înzestrate cu armament nou, destinate să

RAPIDĂ asigure prima ripostă în situaţie de criză şi conflict, să

(F.T.R.R.) participe pe timp de război la îndeplinirea obiectivelor apărării armate a ţării şi să fie întrebuinţată în cadrul structurilor multinaţionale în operaţii militare altele decât războiul.

FORŢE centrele de mobilizare (I., Tc., Art.At., Art.AA., Ge.,

TERÈSTRE DE Po., Nv.Tp.Flv., Pşt. N.B.C., Ce., Trs.) destinate pentru REZERVĂ realizarea capacităţii de acţiune la război.

(F.T.R.)

FORŢE grupare de forţe constituită din mari unităţi şi unităţi de

TERESTRE DE artilerie, artilerie antitanc, artilerie antiaeriană, geniu, SPRIJIN (F.T.S.) apărare N.B.C., transmisiuni şi acţiuni psihologice, destinată pentru sprijinul Forţelor Terestre de Reacţie Rapidă.

FORŢE unităţi, subunităţi şi formaţiuni de cercetare, război

TERESTRE DE electronic şi cercetare radio, radiolocaţie, transmisiuni, SUPRAVEGHERE control N.B.C şi acţiuni psihologice, destinate pentru ŞI AVERTIZARE descpoerirea, identificarea, localizarea şi determinarea TIMPURIE momentului de acţiune a factorilor de risc la adresa

(F.S.A.T.) apărării naţionale.

FORŢE centrele de instrucţie şi mobilizare (Mc., Tc., V.M., Art.,

TERESTRE Art.A.T., Trs.) destinate pentru amplificarea capacităţii

PRINCIPALE de reacţie a Forţelor Terestre în situaţii de criză sau război, (F.T.P.) asigurarea condiţiilor pentru executarea mobilizării şi constituirea forţelor de rezervă.

G

GESTIONAREA ansamblul măsurilor şi acţiunilor de izolare – blocare a UNEI CRIZE conflictelor care alimentează criza (conflictul).

GRUPAREA DE elementul principal al dispozitivului, destinat pentru ANGAJARE îndeplinirea scopurilor operaţiei prin producerea de pierderi cât mai mari, slăbirea treptată a capacităţii de luptă a grupărilor de forţe ale inamicului, oprirea ofensivei acestora şi crearea condiţiilor necesare pentru trecerea la ofensivă.

GRUPAREA DE se constituie din mari unităţi de arme întrunite din forţele de angajare ulterioară, mari unităţi regrupate de pe

CONTRALOVI- direcţiile unde agresorul nu acţionează cu forţe puternicc TURĂ şi, în situaţii deosebite, din rezervă. Valoarea forţelor

(CONTRAATAC) pentru contralovitură trebuie să asiguic superioritatea pe direcţia ripostei ofensive şi succesul acesteia.

GRUPARE un sistem de Torţe de natură şi de volum foarte diverse,

INTERARME constituit temporar sau pemanent în cadrul unei categorii distincte de forţe ale armatei în vederea îndeplinirii unei misiuni comune.

GRUPARE acea grupare de forţe şi mijloacc, pn\.um şi posibilităţile

OPERAŢIONALĂ de loc şi mişcare ale acesteia, carc eslc destinată îndeplinirii unei anumite misiuni, la un moment dat, în strânsă corelare cu situaţia creată.

I

IMAGOLOGIE ramură a sociopsihologiei care cercetează sistematic reprezentările pe care le au popoarele sau clasele sociale despre ele însele.

INSTRUCTOR cadru militar/militar angajat pe bază de contract/gradat, competent pentru a instrui un individ

sau grup de indivizi din structurile armate.

INSTRUIREA ^ proces care constă în ridicarea nivelului de cunoştinţe PENTRU LUPTĂ militare şi de specialitate; perfecţionarea deprinderilor A necesare îndeplinirii atribuţiilor funcţionale; închegarea

COMANDAMEN- acţiunii elementelor componente pentru a asigura TELOR/ funcţionarea acestor tipuri de structuri în concordanţă

COMEZILOR cu misiunile care le revin în situaţii de pace, de criză sau război.

INSTRUMENTELE mijloacele care ajuta în mod intrinsec la realizarea în practică a unei tehnici, metode sau procedeu.

INSTRUCŢIA totalitatea activităţilor de pregătire a resursei umane ARMATEI pentru înzestrarea acesteia cu competenţe, potrivit sarcinilor şi responsabilităţilor funcţionale care să o facă să acţioneze eficient în structurile militare existente şi din care face parte.

INSTRUCŢIA forma de instrucţie care se execută începând cu COLECTIVĂ subunitatea de cel mai mic nivel, respectiv grupa, echipa/

similare, terminând cu unitatea şi care are drept scop însuşirea cunoştinţelor şi formarea deprinderilor necesare acţiunii întrunite a acestora, având două componente: una comună tuturor armelor şi una specifică.

Este condusă de comandamentul nemijlocit al eşalonului care se instruieşte şi se execută numai în perioada instrucţiei subunităţilor şi unităţilor şi numai de către acele structuri militare încadrate cu efective complete.

INSTRUCŢIA w formă de instrucţie care se execută în scopul însuşirii INDIVIDUALĂ cunoştinţelor şi formării deprinderilor generale de militar, de luptător şi specialist în armă, fiind condusă direct de comandantul nemijlocit, prin aplicarea metodelor de instruire specifice tehnicilor rapide de pregătire profesionalizată a trupelor.

INSTRUCŢIA forma de instrucţie care asigură pregătirea subunităţilor/ INTEGRATĂ unităţilor în vederea

îndeplinirii misiunilor de luptă, împreuna cu forţe şi mijloace aparţinând celorlalte structuri militare, arme sau categorii de forţe ale armatei pe care le primeşte ca întărire, în sprijin sau cu care cooperează, în scopul realizării unităţii de conducere şi acţiune.

INSTRUCŢIA w forma de instrucţie care vizează pregătirea subunităţilor/ OPERAŢIONALĂ unităţilor/formaţiunilor, pentru îndeplinirea unor misiuni specifice pe teritoriul naţional/în afara acestuia şi se execută din momentul nominalizării acestora până la data stabilită prin ordin să fie operaţionale.

INSTRUCŢIA w totalitatea activităţilor de instrucţie a militarilor, PENTRU LUPTĂ subunităţilor, unităţilor, marilor unităţi, comandamentelor A ARMATEI şi statelor majore, desfăşurate în scopul însuşirii cunoştinţelor necesare pregătirii şi ducerii luptei, formării deprinderilor de utilizare eficientă a tehnicii militare din dotare şi de conducere a structurilor militare din subordine pentru îndeplinirea misiunilor ce le revin la pace, în situaţii de criză sau la război. Instrucţia pentru luptă a armatei mai cuprinde şi latura teoretică şi practică a pregătirii necesare acţiunilor nonviolente de tipul asimetric (armată contra grupuri neorganizate după tipologia militară) specifice situaţiilor de pace şi criză, precum şi formarea capabilităţilor acţionale necesare intervenţiei la calamităţi şi dezastre.

INSTRUCŢIA forma de instrucţie care se vizează pregătirea în comun a

PENTRU subunităţilor/unităţilor cu structuri similare aparţinând

OPERAŢII armatelor statelor partenere, pentru îndeplinirea unor

INTEGRATE misiuni specifice de meţinere a păcii, căutare-salvare,

MULTINA- umanitare. ŢIONALE

INSTRUCŢIA forma de instrucţie care vizează pregătirea subunităţilor SPECIALA A şi unităţilor în vederea îndeplinirii misiunilor de luptă ARMEI specifice

fiecărei arme.

INTEGRALITATE concertarea instrucţiei în scopul obţinerii „luptătorului performant”, abil mânuitor al mijloacelor de luptă, cu mentalitate de învingător, eficient în situaţii limită, capabil de autocontrol, adept al spiritului de echipă, cooperant şi excelent camarad.

INTEROPERABI- capacitatea comandamentelor şi forţelor ţărilor partenere LITATE de a acţiona în comun cu cele ale ţările membre NATO.

INTEROPERABI- capacităţilor sistemelor unităţilor, subunităţilor şi LITATEA formaţiunilor de logistică de a furniza servicii către şi de

LOGISTICĂ a accepta servicii de la alte sisteme şi forţe de logistică de acelaşi fel şi de a utiliza serviciile astfel schimbate, pentru a le face capabile să opereze efectiv împreună.

L

LEGEA obiectivele şi misiunile trebuie astfel stabilite încât să

CONCORDANŢEI corespundă posibilităţilor acţionale ale forţelor şi DINTRE mijloacelor avute la dispoziţie. Exigenţele legii implică

SCOPURI, o analiză temeinică şi multilaterală a situaţiei, a cantităţii

FORŢE ŞI şi mai ales a calităţii forţelor şi mijloacelor de care se

MIJLOACE dipune pentru stabilirea, pe baze realiste, a grupărilor de forţe şi mijloace necesare nimicirii inamicului.

LEGEA exprimă necesitatea adoptării unor noi procedee şi chiar

DEPENDENŢEI forme de luptă care să corespundă caracteristicilor

FORMELOR ŞI tehnico-tactice ale armamentului nou introdus în

PROCEDEELOR înzestrarea armatei şi schimbărilor calitative ce apar în

ACŢIUNILOR domeniul tehnicii de luptă.

MILITARE DE
NIVELUL
DEZVOLTĂRII
ARMAMENTULUI
SI TEHNICII DE
LUPTĂ

LEGILE LUPTEI raporturi esenţiale, obligatorii, generale, caracterizate prin ARMATE repetabilitate şi stabilitate relativă între componentele interne ale fenomenului militar, precum şi între acestea şi alte domenii sociale, care determină pregătirea şi desfăşurarea acţiunilor militare.

LEGEA condiţioaneză obţinerea succesului în lupta de realizare

RAPORTULUI a unei superiorităţi de forţe şi mijloace faţă de adversar DE FORŢE în raioanele şi pe direcţiile cele mai importante. În esenţă exprimă relaţia dintre cantitatea şi calitatea forţelor şi mijloacelor părţilor care se înfruntă prin luptă armată, relaţie exprimată cu un grad ridicat de probabilitate.

LEGEA exprimă conexiunea luptei armate din toate mediile î

UNITĂTII care se desfăsoară.

ACŢIUNILOR

LIBERTATEA DE asigurarea condiţiilor de autonomie în decizie, ACŢIUNE planificarea şi desfăşurarea acţiunilor proprii şi de limitare, pnă la anihilare, a posibilităţilor de opţiune şi acţiune ale inamicului.

LOGISTICA un complex de măsuri şi acţiuni desfăşurate pentru asigurarea condiţiilor materiale necesare pregătirii şi ducerii acţiunilor militare.

LOGISTICA un complex de măsuri şi activităţi desfăşurate pentru

FORŢELOR aprovizionarea forţelor destinate ducerii acţiunilor

TERESTRE militare, transportul, mentenenţa, asigurarea medicală, sanitar-veterinară financiară a căilor de comunicaţie, cartiruirea trupelor şi adăpostirea

animalelor pentru îndeplinirea misiunilor ce-i revin acestor categorii de forţe ale armatei pe timp de pace, în situaţii de criză şi la război.

LOGISTICA totalitatea activităţilor desfăşurate de organele de

INSTRUCŢIEI specialitate şi abilitate pentru asigurarea bazei materiale şi tehnice necesare desfăşurării instrucţiei, conform normelor de echipare, cazare, hrănire şi dotare cu tehnică a structurilor în strânsă concordanţă cu posibilităţile bugetare are Ministerului Apărării Naţionale.

LOGISTICA totalitatea activităţilor ce se desfăşoară în scopul asigurării

TRUPELOR marilor unităţi, unităţilor şi subunităţilor cu tot ceea ce le este necesar pentru pregătirea şi ducerea acţiunilor.

LOVITURA constă dintr-o puternică pregătire de foc, după care trupele

FRONTALĂ rup apărarea inamicului, pătrund în adâncimea dispozitivului acestuia executând concomitent manevre de învăluire pentru încercuirea şi nimicirea pe părţi a adversarului. Se execută pe una sau mai multe direcţii, de regulă acolo unde apărarea inamicului este mai slabă.

LOVITURA ÎN o formă de manevră în cadrul operaţiei ofensive, care ADÂNCIME presupune constituirea unor puternice grupări de manevră capabile să pătrundă în adâncimea dispozitivului inamicului în scopul lovirii decisive a obiectivelor importante de pe direcţiile de ofensivă, acţionând concomitent cu forţele care lovesc frontal inamicul.

LOVIREA DE constă în acţiunea simultană a unor grupări de forţe

DIRECŢII separate, pe direcţii care converg spre obiective

CONVERGENTE importante din dispozitivul inamicului.

LUCRUL ÎN presupune eforul operativ al membrilor

unui grup pentru

ECHIPĂ realizarea unor scopuri comune; încredere şi confidenţialitate; delegare de autoritate/competenţă şi cooperare în cadrul echipei.

LUPTA confruntarea armată sau un şir de confruntări prin care se urmăreşte îndeplinirea unor scopuri de importanţă tactică.

LUPTA w confruntarea militară violentă între două forţe adverse

ARMATĂ cu putere de luptă şi care urmăresc, fiecare în parte, îndeplinirea scopurilor propuse.

LUPTA DE procedeul prin care două grupări de forţe adverse, în

ÎNTÂLNIRE mişcare din sensuri opuse, angajează lupta urmărind realizarea scopurilor propuse prin acţiuni ofensive.

LUPTĂTOR persoană dotată fizic, intelectual, moral şi psihic care poate duce acţiuni de luptă individuale sau în cadrul unui colectiv (structură militară) la cele mai înalte standarde.

M

MANAGENTUL procesul de prevenire, limitare sau soluţionare a crizelor.

CRIZEI El stabileşte procedurile şi activităţile planificate şi desfăşurate pentru a aduce criza sub controlul celor care o gestionează, pentru a le permite acestora, ca prin acţiunile lor, să oprească evoluţia ei următoare.

MANEVRA ansamblul acţiunilor prin care se urmăreşte realizarea î ascuns a celei mai corespunzătoare grupări de forţe şi mijloace în locul şi la timpul stabilit şi punerea lor într-o situaţie favorabilă pentru executarea unor lovituri hotărâtoare asupra inamicului sau pentru sustragerea forţelor proprii de sub loviturile acestuia.

MANEVRA DE constă în fixarea şi angajarea de front a inamicului cu o

ÎNTOARCERE parte din forţe, iar cu gruparea principală acţionându-se în flancul şi spatele dispozitivului

acestuia, pe o adâncime cât mai mare, cu interceptarea comunicaţiilor pentru interzicerea acţiunilor forţelor inamicului care se retrag şi ale rezervelor sale ce afluiesc din adâncime. Se adoptă în scopul nimicirii întregii grupări de forţe ale inamicului.

MANEVRA DE constă în executarea unor lovituri care să conducă rapid ÎNVĂLUIRE în flancul şi în spatele forţelor principale ale inamicului pătruns pe teritoriul naţional, alegându-se în general locurile cele mai slabe ale dispozitivului acestuia (intervale, flancuri, goluri), în scopul nimicirii lui pe părţi într-un timp relativ scurt.

MANEVRA DE o formă de manevră care se aplică pentru nimicirea DIRECŢII succesivă sau pe părţi a grupărilor inamicului. Se adoptă

INTERIOARE atât în ofensivă cât şi în apărare, atunci când inamicul (DIN POZIŢIE acţionează cu mai multe grupări, iar forţele proprii se CENTRALA) găsesc într-o poziţie centrală şi nu pot face faţă concomitent grupărilor acestuia.

MARŞUL deplasarea organizată a structurilor militare pe vehicule proprii (tehnică blindată) sau pe jos (schi).

MASCAREA ansamblul de măsuri şi acţiuni care se planifică şi se desfăşoară pentru ascunderea elementelor dispozitivului şi a activităţilor trupelor proprii faţă de concentrarea de toate categoriile a inamicului, precum şi pentru inducerea în eroare a acestuia asupra situaţiei, intenţiilor, acţiunilor şi posibilităţilor trupelor proprii în timp şi spaţiu.

MENTENANTĂ totalitatea măsurilor întreprinse pentru a menţine sau a restabili starea de utilizare/funcţionare a materialelor şi a tehnicii la parametrii specifici, acestea incluzând inspectarea, tratarea, service-ul (întreţinerea+reparaţiile curente), stabilirea categoriei, reparaţiile, refacerea, recondiţionarea/modernizarea.

MENŢINEREA efortul de căutare a păcii de către părţile implicate şi de PĂCII către unii terţi interesaţi,

contribuind totodată la gestionarea unui conflict.

METODA determină rezolvarea simultană a unor paşi, prin delegare

CONDUCERII de competenţă, concomitent cu creşterea eficacităţii

PRIN elementului condus. OBIECTIVE

METODA constă în realizarea transferului de cunostinte prin

INSTRUIRII ÎN parcurgerea etapei intuiţiei vn şi pregătim aperceptive

PUNCTE DE sub conducerea directă şi nemijlocită a instructorului în

BAZĂ vederea iniţierii şi formării corecte a deprinderilor de bază ale luptătorului individual sau colectiv.

METODA constă în parcurgerea de către fiecare luptător în mod

PREGĂTIRII ÎN individual, prin procedeul autoinstruirii/descoperirii PUNCTELE următoarelor etape psihopedagogice de învăţare şi

PERMANENTE instruire: Însusirea teoretică şi învăţarea practică;

recunoaşterea şi comparaţia; sintetizarea şi reproducerea; uitarea şi memorarea remanentă; execuţia şi corecţia secvenţială; exersarea şi automatizarea; antrenamentul şi perfecţionarea, în scopul realizării transferului de cunoştinţe, capabilităţi psiho-motrice şi acţionale necesare îndeplinirii misiunilor de luptă.

METODĂ DE modalitatea prin care conducătorul militar consideră că CONDUCERE se poate îndeplini misiunea cu eficienţă maximă.

Viabilitatea acesteia se determină prin analiza raportului dintre obiectivul de îndeplinit şi costurile obţinute.

MODELUL arhitectura ideală care integrează într-un tot unitar competenţele cu care trebuie să fie înzestrat agentul acţiunii militare pentru a corespunde rolurilor şi funcţiilor create în cadrul structurilor militare.

MORALUL ansamblul stărilor de spirit succesive ale militarilor în

(MILITARILOR) legătură cu îndeplinirea unor activităţi specifice armatei, având ea determinări obiective dimensiunile cadrului sociomaterial al activităţii militare (instrucţie sau luptă), ca sursă psihologică.

MULTIDISCIPLI- presupune formare şi dezvoltarea luptătorului complet, NARITATEA cu un important grad de autonomie acţională în îndeplinirea misiunilor de luptă.

O

OBIECTIVELE finalităţile/ ceea ce urmează să fie realizat, către care INSTRUCŢIEI este orientată întreaga activitate de instrucţie.

OBIECTIVUL formarea, specializarea şi perfecţionarea succesivă a FUNDAMENTAL cadrelor militare active şi în rezervă ca profesionişti AL autentici, cetăţeni culţi, cu o aleasă educaţie patriotică,

ÈWATAMÂNIULUI morală şi civică, în spiritul tradiţiilor omeniei şi MILITAR demnităţii, specialişti cu temeinice cunoştinţe, priceperi şi deprinderi în domeniile necesare Forţele Terestre, cu profunde convingeri şi corecte atitudini faţă de valorile supreme ale statului de drept, capabile să-şi îndeplinească atribuţiilor ce le revin la pace, în situaţii de criză şi război.

OBIECTIVUL dezvoltarea capacităţii structurilor de comandă de a PRINCIPAL AL conduce acţiuni militare în situaţii complexe şi realizarea INSTRUCŢIEI unui nivel ridicat de instruire a structurilor acţionale.

FORŢELOR TERÉSTRE

OPERATIV care lucrează repede, expeditiv, activ; termenul se asociază direct sau indirect unei acţiuni care este dorită să se desfăşoare cât mai repede, cu o eficienţă cât mai apropiată de scopul propus, deci cu rezultate finale favorabile.

OPERATIVITATE calitatea de a fi operativ, calitate a conducerii trupelor concretizată în rapiditate şi eficienţă în reculegerea, prelucrarea şi transmiterea informaţiilor (ordinelor, dispoziţiilor) necesare conducerii acţiunilor de

luptă.

OPERAŢIA ansamblul de acţiuni militare complexe, desfăşurate unitar, în mediul terestru, aerian, maritim sau fluvial, prin care se urmăreşte îndeplinirea unor scopuri de importanţă operativă sau strategică.

OPERAŢIA DE ansamblul acţiunilor desfăsurate de forţe întrunite cu rol APĂRARE strategic sau operativ, într-un spaţiu geografic (fâşie, zonă), care include cel puţin o direcţie de interes sau un obiectiv de menţinut, prin care se asigură îndeplinirea unor scopuri parţiale ale operaţiei de nivel strategic.

OPERAŢIA totalitatea acţiunilor duse de o grupare de forţe cu rol

ÎNTRUNITĂ strategic sau operativ, constituită din trupe aparţinând mai multor categorii de forţe armate, sub comandă unică, în mediul corespunzător fiecăruia, dar cu un scop unitar.

OPERAŢIA ansamblul acţiunilor desfăşurate de forţe cu rol strategic

OFENSIVĂ (operativ) într-un spaţiu geografic (zonă, fâşie) ce include cel puţin o direcţie sau un obiectiv, prin cucerirea cărora se realizează unul sau mai multe scopuri parţiale ale apărării armate a ţării (operaţiei de nivel strategic).

OPERAŢIA acţiunea dusă de o grupare de forţe terestre cu rol operativ

TERESTRĂ sau strategic, independent sau în cooperare cu grupări de forţe din celelalte categorii de forţe ale armatei, după un plan unic, cu scopul de a apăra sau cuceri obiective terestre de importanţă operativă sau strategică.

OPERAŢII DE acţiuni destinate să demonstreze hotărârea României, „ARĂTĂRE”/ implicând o activitate crescută a forţelor sale dislocate, EXPUNERE A în încercarea de a dezamorsa o situaţie specifică, care, FORŢEI dacă ar continua, ar periclita interesele sau obiectivele naţionale.

OPERAŢII DE operaţii desfăşurate pentru căutarea,

localizarea,

CĂUTARE- identificarea, salvarea şi recuperarea personalului, a

SALVARE echipamentului sensibil sau materialelor importante

(RECUPERARE) pentru securitatea naţională.

OPERAŢII DE acele acţiuni desfăşurate pentru a evacua noncombatanţii EVACUARE A aflaţi sub ameninţare, dintr-o ţară străină. Aceste operaţii NONCOMBA- implică în mod normal cetăţeni ai României sau a unei TANŢILOR naţiuni aliate, a căror viaţă este în pericol şi pot implica totodată evacuarea selectivă a cetăţenilor naţiunii gazdă precum şi cetăţenilor altor ţări.

OPERAŢII DE operaţii de folosire a forţei militare sau de ameninţare cu IMPUNERE A acesta, desfăşurate în conformitate cu rezoluţiile şi PĂCII sancţiunilor destinate menţinerii sau restabilirii păcii şi ordinii.

OPERAŢII DE operaţii militare desfăşurate cu acordul tuturor părţilor MENŢINERE A implicate, în scopul monitorizării şi implementării unui PĂCII acord urmărindu-se instaurarea unei stabilităţi politice de perspectivă.

OPERAŢII activităţi în care instrumentul militar al puterii naţionale

MILITARE a este folosit pentru scopuri altele decât varietatea ALTELE DECÂT operaţiilor însumate/asociate războiului, care urmăresc RĂZBOIUL descurajarea războiului, rezolvarea conflictului, promovarea păcii şi sprijinul autorităţilor civile în vederea soluţionării crizelor interne.

OPERAŢII operaţii conduse de forţe aparţinând mai multor naţiuni

MULTINAŢIO- care acţionaează împreuna pentru îndeplinirea unei singure NALE misiuni.

OPERAŢIONAL ceva sau cineva pregătit să intre în acţiune (activitate, operaţie); capacitatea optimă a formaţiunilor (grupurilor, colectivelor) de a putea fi angajate în operaţie.

OPERAŢIONALI- proprietatea de a interveni prompt în rezolvarea unei TĂTE probleme; calitatea organismelor de conducere

(comandamente militare) de a fi capabile ca într-un termen relativ scurt să rezolve pe baza unor decizii, problemele multiple – atât în plan conceptual cât şi acţionai, pe timpul pregătirii şi desfăşurării acţiunilor militare.

OPERAŢIONALI- întreprinderea unui summum de operaţii, adică ZARE totalizarea, cuantificarea şi evaluarea lor alături de nişte parametri la care trebuie să se ajungă pentru ca sistemele de conducere subordonate să devină operaţionale.

OPERAŢIONALI- principiu care asigură, prin aplicare sa, instrumentele prin ZAREA care factorii de decizie politico-militară pun în mişcare

STRUCTURILOR sistemul, pentru a atinge pragul de reacţie într-un interval de timp cât mai scurt.

OPERAŢIUNE acţiune militară de sprij inire a eforturilor diplomatice ale DE PACE comunităţii internaţionale pentru impunerea, menţinerea sau restabilirea păcii şi a securităţii în zonele de conflict.

ORDINE w starea în care se găseşte ordinea publică într-un stat la

OONSmunONALA un moment dat, modul de desfăşurare a tuturor activităţilor şi acţiunilor politice, sociale, economice şi militare, având la bază Constituţia şi legile ţării, respectiv modul în care sunt apărate drepturile omului şi sunt executate îndatoririle cetăţeneşti în vederea aigurării viabilităţii statului de drept.

ORGANIZAREA funcţie a conducerii care semnifică folosirea judiciaosă a resurselor umane şi materiale în rezolvarea unor probleme concrete, utilizarea eficientă a resurselor; presupune armonizarea, stabilirea unor raporturi şi proporţii juste între categoriile de resurse.

ORGANIZAREA ansamblul de activităţi prin intermediul cărora se stabilesc INSTRUCŢIEI sarcinile, pe structuri şi posturi, necesare realizării ARMATEI

obiectivelor propuse şi are menirea de a pune în valoare următoarelor concepte: autoritatea, responsabilitatea, centralizarea sau descentralizarea sistemului de instrucţie.

P

PARTICIPAREA misiuni care se realizează prin pregătirea în cadrul unor LA APĂRAREA exerciţii cu participare internaţională la acţiuni COMUNĂ multinaţionale şi interaliate, precum şi în structura unor mari unităţi şi unităţi mixte, în scopul sporirii măsurilor de încredere şi de securitate.

PERIOADĂ DE intervalul de timp în care inamicul potenţial desfăşoară, TENSIUNE de regulă, acţiuni complexe de intimidare a statului român, concomitent cu obţinerea acordului şi a sprijinului internaţional faţă de poziţia şi revendicările sale.

PLAN document organizatoric necesar unei activităţi militare importante şi complexe, cuprinzând totalitatea măsurilor de trebuie adoptate pentru atingerea obiectivelor fixate.

PLANIFICAREA funcţie a conducerii care reprezintă un ansamblu de acţiuni de complexitate variabilă, întreprinse în vederea determinării cât mai clar posibil a tuturor elementelor ce caracterizează activitatea (procesul) condus şi anume: obiective, subiect resurse (umane, materiale, financiare, informaţionale), probleme de spaţiu, timp, instrumente, metode şi procedee utilizate. Reprezintă, de asemenea, stabilirea şi fundamentarea obiectivelor şi sarcinilor de realizare a acestora precum şi a resurselor necesare pe o perioadă determinată, corespunzătoare obiectivului urmărit – lunar, trimestrial, anual.

PLANIFICAREA stabilirea obiectivelor şi direcţiilor de acţiune în mod INSTRUCŢIEI concret pe o anumita perioadă de timp în vederea folosirii ARMATEI eficiente a tuturor resurselor care stau la baza funcţionării programului de instrucţie a armatei.

PLURIFUNCŢIO- realizarea instrucţiei polivalente a militarului care să-i NALITATE transfere capabilităţi

acţionale eficiente necesare îndeplinirii mai multor funcţiuni/posturi specifice armei/ specialităţii militare.

POTENŢIAL termen care defineşte ceva, care are în sine toate condiţiile esenţiale pentru realizare, care există ca posibilitate, care există în mod virtual.

POTENŢIAL totalitatea forţelor şi mijloacelor de luptă armata pe care

MILITAR un stat le poate afecta pregătirii şi ducerii războiului.

PREDICŢIE formulare de enunţuri ce descriu desfăşurarea probabilă a unor fenomene şi evenimente în virtutea cunoaşterii dinamicii comportamentelor acestora.

PREGĂTIREA un ansamblu de activităţi şi măsuri ce se execută de ACŢIUNILOR comandamente şi de forţele subordonate acestora pentru MILITARE conceperea şi planificarea acţiunii, organizarea asigurării acţiunilor şi protecţiei trupelor şi logisticii, aducerea forţelor şi mijloacelor la capaciteatea de luptă necesară şo în dispozitivele şi situaţiile optime, realizarea coordonării permanente a subordonaţilor şi a cooperării neîntrerupte între toate forţele participante.

PREGĂTIREA totalitatea acţiunilor de lovire ale aviaţiei, artileriei, DE FOC A rachetelor şi altor mijloace de foc executate în mod unitar,

ATACULUI prin surprindere, într-o perioadă de timp stabilită, în scopul nimicirii sau neutralizării inamicului, îndeosebi în sectoarele de rupere şi pe direcţiile de ofensivă ale marilor unităţi.

PREGĂTIREA totalitatea acţiunilor categoriilor şi sistemelor de DE FOC A armamente şi mijloace de lovire (aviaţie, artilerie şi

OFENSIVEI rachete antiaeriene, artileria de pe navele maritime şi fluviale, tancuri) executării în scopul diminuării puterii de luptă şi anihilării acţiunilor inamicului în spaţiul terestru, maritim, aerian şi fluvial, în special pe direcţiile de ofensivă. Aceasta se realizează astfel încât să se asigure lovirea la distanţa mixímă posibilă a mijloacelor de întrebuinţare a armelor de

nimicire în masă, sistemelor de cercetare-lovire de înalta precizie, punctelor de comandă şi a grupărilor de forţe inamice aflate în raioane sau în deplasare.

PREVEDERE deducere, intuire, întrezărire, bizuire asupra evoluţiei probabile a unui fenomen în perspectivă.

PREVENIREA, misiune care, în principal, vizează avestizarea populaţiei, INLATURAREA pregătirea acesteia pentru acţiune în diferite situaţii, ŞI LICHIDAREA elaborarea planurilor de evacuare şi participarea cu forţe URMĂRILOR şi mijloace la înlaturarea efectelor dezastrelor. DEZASTRELOR

PREVENIREA activităţi care pornesc de la iniţiativele diplomatice şi CONFLICTELOR până la desfăşurarea preventivă a trupelor, în scopul prevenirii escaladării disputelor spre o fază superioară, aceea a conflictelor armate sau prevenirii extinderii disputelor.

PREVIZIUNE prevedere întemeiată pe cunoaşterea legilor obiective care guvernează evoluţia probabilă a respectivului fenomen în perspectivă.

PREVIZIUNEA analizarea resurselor disponibile şi gestionarea acestora SISTEMULUI în vederea stabilirii obiectivelor în domeniul instrucţiei MANAGERIAL armatei pe o perioadă de timp determinată având ca AL INSTRUCŢIEI scopuri: stabilirea obiectivelor şi scopurilor propuse;

stabilirea sarcinilor şi atribuţiilor pe structurile ce compun sistemul; stabilirea orientărilor şi modul de coordonare a activităţilor de instruire în cadrul sistemului; prevederea disfuncţionalităţilor ce pot apare în cadrul sistemului şi măsurile corective ce trebuie adoptate pentru eliminarea acestora; stabilirea sistemului de control şi modul de aplicare a prevederilor acestuia pentru îndeplinirea obiectivelor propuse.

PREZENŢA totalitatea activităţilor care demonstrează angajarea

ÎNAINTATA Armatei Române pentru consolidarea stabilităţii regionale, conferă credibilitate alianţelor din care România face parte şi sporesc posibilităţile de

răspuns în cazul unei crize.

PRIMATUL determină un anumit tip de ripostă a Forţelor Terestre,

LOVITURII prin care se urmăreşte ca pe timpul desfăşurării acţiunilor militare, în anumite circumstanţe ale situaţiei operative care favorizează trupele proprii, să se execute lovituri decisive, preventive şi prin surprindere, cu forţe strict limitate pentru devansarea şi surprinderea în acţiune a adversarului.

PROCEDEU prescripţie privind ordinea operaţiilor succesive de abordare a proceselor şi fenomenelor în vederea organizării formale a datelor obţinute şi activităţilor.

PROCEDEU DE modelul/felul de efectuare/executare a instructiei.

INSTRUCŢIE

PROCEDURĂ totalitatea măsurilor, activităţilor şi documentelor

DE STAT elaborate/executate succesiv, pentru a ajunge la o decizie

MAJOR sau pentru a îndeplini o decizie din procesul executării actului de comandă.

PROGNOZA activitatea de cunoaştere şi investigare în timp a etapelor

INSTRUCŢIEI pe care urmează să le parcurgă procesul de instrucţie,

ARMATEI având ca rezultat stabilirea obiectivelor de perspectivă şi fundamentarea deciziilor în acest scop, în strânsă concordanţă cu evoluţia fenomenului militar mondial.

PROGNOZĂ prevedere a desfăşurării în timp a unui fenomen, a unui proces etc., bazată pe studiul împrejurărilor care îi determină apariţia şi evoluţia; prevedere a valurilor pe care le vor lua în viitor unele mărimi din prezent.

PROGRAMARE documente care cuprind obiectivele pe arme, categorii

DE INSTRUCŢIE de instrucţie, teme, exerciţii şi

şedinţe, atât la nivelul luptătorului cât şi al subunităţilor/unităţilor, procedeele, regulile, standardele, resursele alocate precum şi etapele/ perioadele/modulele şi responsabilităţile privind conducerea şi executarea instrucţiei.

PROTECŢIA ansamblul de măsuri şi acţiuni desfăşurate continuu şi într-o concepţie unitară, de către toate forţele participante şi la toate eşaloanele, destinate creării condiţiilor de securitate a personalului, tehnicii şi sistemelor împotriva acţiunilor agresorului şi a altor factori perturbatori, executate în scopul menţinerii capacităţii de luptă a trupelor şi îndeplinirii misiunilor primite.

PROTECŢIA w ansamblul măsurilor şi acţiunilor întreprinse pentru

ANTIAERIANĂ prevenirea şi apărarea grupărilor de forţe şi a obiectivelor proprii împotriva cercetării aeriene şi a loviturilor executate din aer de către agresor incusiv prin folosirea mijloacelor nespecializate de luptă împotriva ţintelor aeriene.

PROTECŢIA ^ ansamblul măsurilor şi acţiunilor desfaşurate unitar pentru ELECTRONICĂ asigurarea stabilităţii şi a continuităţii lucrului mijloacelor şi sistemelor electronice proprii. Se realizează prin respectarea regulior şi regimului de lucru electronic propriu, mascarea şi dezinformarea electronică, organizarea compatibiliţii electromagnetice între mijloacele (sistemele) electronice proprii, precum şi prin decoperirea, neutralizarea şi interdicţia utilizării mijloacelor de luptă electronică ale inamicului.

PROTECŢIA ansamblul măsurilor, acţiunilor şi lucrărilor genistice care

GENISTICĂ se planifică şi execută de către toate forţele, în folosul propriu, pe timpul pregătirii şi desfăşurării acţiunilor, pentru crearea condiţiilor necesare adăpostirii şi protejării personalului şi tehnicii împotriva loviturilor de orice gen ale inamicului şi pentru îngreunarea şi interzicerea acţiunii acestuia.

PROTECŢIA ansamblul măsurilor şi acţiunilor organizatorice,

INFORMÂŢIILOR informaţioanle şi tehnice luate şi executate pentru respectarea regulilor de lucru în elaborarea şi exploatarea documentelor, tehnicii şi materialelor de conducere în secret şi pentru păstrarea secretului, accesul autorizat şi ierarhizat la date şi informaţii, controlul informaţiilor destinate publicului, protecţia fizică şi criptografică a informaţiilor ce se transmit, disimularea informaţională a inamicului, penetrarea documentelor de conducere în secret, cifrurilor şi codurilor adversarului.

PROTECTIA ansamblul de măsuri şi acţiuni ce se desfăsoară pentru

ÎMPOTRIVA protecţia personalului împotriva efectelor armelor şi

MIJLOACELOR muniţiilor incendiare, limitarea şi stingerea ingendiilor INCENDIARE în dispozitivul trupelor şi ieşirea din raioanele în care se produc incendii masive.

PROTECŢIA ansamblul măsurilor şi acţiunilor care se stabilesc şi se

MEDICALĂ ŞI desfăşoară în vederea păstrării sănătăţii militarilor şi

SANITAR- ^ animalelor, prevenirii apariţiei şi răspândirii bolilor,

VETERINARĂ inclusiv a celor provocate de armele de nimicire în masă.

PROTECŢIA w ansamblul de măsuri şi acţiuni desfăşurate într-o PSIHOLOGICĂ concepţie unitară, pentru menţinerea rezistenţei şi stabilităţii psihice a efectivelor proprii, ridicarea moralului acestora, identificarea şi constracararea presiunilor psihice care afectează capacitatea de luptă şi pentru influenţarea psihologică a trupelor inamicului.

PUNCTUL DE locul de dispunere a personalului şi mijloacele COMANDĂ comandamentului din care se exercită actul de comadă pe timpul pregătirii şi desfăşurării acţiunilor militare-PUNCTUL DE se poate crea

pentru o perioadă de timp determinată COMANDĂ ales la eşalonul corp de armată, în vederea conduceri1

AJUTĂTOR unei grupări de forţe ce acţionează pe o direcţie izolai-PUNCTUL DE este destinat pentru întărirea stabilităţii, siguranţei $ COMANDĂ DE continuităţii conducerii trupelor. El trebuie să fie pregâtţ1 REZERVĂ pentru a prelua imediat şi integral conducerea în cazul scoate^

din funcţiune sau a deplasării punctului de comandă.

PUTEREA DE componentă esenţială a copacităţii combative spécifié LUPTĂ structurilor militare, exprimată integrator prin element*^

capacităţii de distrugere a adversarului (puterea de loviri conducerea, manevra, reacţia şi protecţia).

PUTEREA^ una din componentele importante ale puterii militare a

MILITARĂ A României, determinată în mod direct de posibilităţii FORŢELOR naţiunii de a o amplifica, regenera şi redimensiona la

TERÉSTRE nevoie. Se identifică prin: locul şi rolul, efectivele

(personalul militar), armamnetul şi tehnica militar^ structura organizatorică, coeziunea forţelor, starea S1 practica disciplinară, pregătirea pentru lupta a trupel°r şi capacitatea comandamentelor de a gândi, planific opera şi acţiona întrunit, inclusiv în structurii multinaţionale.

R

RAIDUL o operaţie mai restrânsă care impUcă o pătrundere rapid*

În teritoriul ostil pentru obţinerea de informaţi1» dezorientarea adversarului sau distrugerea unor obiective şi se încheie cu o retragere planificată.

RĂZBOI fenomen politico-militar care reprezintă forma cea violentă de manifestare a relaţiilor conflictuale existente la un moment dat între grupări mari de oameni (popoare, naţiuni, state, coaliţii de state, comunităţi sociale, etnice» religioase) organizate din punct de vedere militar, care folosesc lupta armată pentru atingerea

scopuri^ urmărite, ceea ce conferă acestui fenomen un puternic caracter distructiv.

p WnoT n a câp ^ r^zboi în care nu se folosesc armele de nimicire în

J™ ™^^?^ masă ci numai mijloacele de luptă clasice. Lupta de suce

((JUINVtiviâuiNal.) numai cu forţe armatc rcgulatCt deosebindu-se în acest fel de războaiele duse cu forţe armate neregulate (miHtf1* guerile. Oartizani etc Y

RĂZBOI DE concepţie de ducere a războiului care nu presupune

INTENSITATE victoria, ci reducerea graduală a violenţei printr-un REDUSĂ control relativ al conflictului pe baza unui instrument pluridimensional social.

RĂZBOI tip de război prin care se încearcă evitarea riscurilor şi

LIMITAT consecinţelor unui război nuclear total, întroducându-se o serie de limitări în ceea ce priveşte scopurile urmărite, armele întrebuinţate şi teatrul de acţiuni militare.

RĂZBOI tip de război în care predomină acţiunile manevriere,

MANEVRIER fiecare dintre beligeranţi urmărind obţinerea deciziei prin (DE MIŞCARE) operaţii cu caracter mobil.

RĂZBOI acel conflict armat care adoptă principii noi, ca rezultat

MODERN al unor interdependenţe între evenimentele de natură conflictuală, apariţia unor noi armamente şi tehnici de luptă şi, în sfârşit, o alegere sau o compunere a acţiunilor, altele decât în războaiele desfăşurate sau în curs de desfăşurare.

RĂZBOI tip de război preconizat să se desfăşoare cu efective reduse

PUTERNIC (profesionişti), înzestrate cu sisteme de armament şi

DEMASIFICAT tehnică de luptă moderne, performante.

RĂZBOI TOTAL tip de război în care se urmăreşte distrugerea totală a adversarului şi se foloseşte în acest scop totalitatea mijloacelor de luptă.

REACŢIE termen prin care se justifică o acţiune rapidă condiţionată

RAPIDĂ de un pretext sau o modalitate de a concepe reacţia unei armate sau a unei grupări de forţe.

REGRUPAREA acţiunea prin care se realizează o nouă grupare a forţelor şi mijloacelor în scopul îndeplirii aceleiaşi misiuni sau a uneia noi.

RELAŢII DE totalitatea activităţilor desfăşurate de structurile

COOPERARE Ministerului Apărării Naţionale într-o concepţie unitară pentru asigurarea resurselor, planificarea, organizarea, îndrumarea, controlul şi evaluarea sistemului de instrucţie al armatei.

RESTABILIREA ansamblul măsurilor şi acţiunilor întreprinse de către ORDINII organele şi forţele legale ale statului destinate pentru

CONSinupONALE repunerea acesteia în drepturile ei fireşti, atunci când a fost grav tulburată.

RESURSA suma alocată armatei din bugetul statului pentru

FINANCIARĂ (A instrucţie, cu implicaţii determinate în planificarea INSTRUCŢIEI) obiectivelor şi scopurilor ce trebuie îndeplinite într-o unitate de timp.

RESURSA ^ totalitatea materialelor pentru instrucţie, a echipa-MATERIALĂ (A mentelor, utilajelor şi tehnicii din dotare, precum şi a INSTRUCŢIEI) infrastructurii necesare instrucţiei (poligoane, piste, servicii etc.) care, palnificate şi folosite în mod judicios constribuie la instrucţia trupelor din structurile armatei, conform programului stabilit.

RESURSA personalul de decizie şi execuţie din sistemul de instrucţie

UMANĂ prin care se asigură realizarea documentelor care stau la baza instrucţiei armatei şi punerea în practică a prevederilor acestora, concomitent cu planificarea şi

gestionarea resurselor materiale şi financiare.

RESURSĂ (A element de bază, fără de care sistemul de instrucţie al INSTRUCŢIEI) armatei nu poate să-şi atingă scopul pentru care a fost înfiinţat şi consta în totalitatea posibilităţilor pe care le are societatea la un moment dat de a pune la dispoziţia armatei efectivele, baza materială şi financiară necesară instrucţiei în conformitate cu obiectivele stabilite.

RESURSE ansamblul forţelor şi mijloacelor specializate pentru lupta

MILITARE armată, pe care staul român le poate destina pregătirii şi ducerii războiului, dacă acesta este impus şi anume: efectivele şi tehnica de luptă; numărul şi calitatea cadrelor de comadă, organizarea şi coeziunea forţelor armate; nivelul pregătirii populaţiei pentru apărare; gradul de dezvoltare a ştiinţei şi artei militare.

RESURSELE totalitatea posibilităţilor umane, financiare, materiale şi

APĂRĂRII de altă natură de care staul român dispune şi pe care le

NAŢIONALE poate angaja în susţinerea efortului de apărare a ţării.

RETRAGEREA procedeul defensiv prin care forţele angajate în luptă întârzie acţiunile inamicului şi se sustrag loviturilor puternice ale acestuia, schimbându-şi poziţiile de luptă spre înapoi.

REZERVA element component al dispozitivului de luptă întrebuinţat pentru rezolvarea unor situaţii critice neprevăzute care pot să apară pe timpul desfăşurării operaţiei. Se constituie din mari unităţi (unităţi), din toate categoriile de forţe ale armatei, din arme şi specialităţi, în funcţie de existentul acestora, complexitatea situaţiilor şi caracteristicile geoclimatice ale zonei.

REZERVE totalitatea resurselor militare, economico-financiare,

STRATEGICE demografice, tehnologice şi materiale care se constituie la nivel statal şi al eşaloanelor militare strategice ce se întrebuinţează în caz de război sau de

criză (catastrofe naturale sau ecologice) în vederea rezolvării unor situaţii neprevăzute sau a amplificării (intensificării) acţiunilor militare în curs de desfăşurare.

RIPOSTĂ ansamblul de acţiuni spaţiale şi acţionale în teritoriul adversarului, care includ totalitatea atitudinilor ofensive, defensive şi pasive ale unei categorii de forţe ale armatei.

RIPOSTĂ o atitudine strategică, o modalitate de a respinge agresiuni

ARMATĂ w armate printr-o apărate strategică flexibilă şi activă, în

DEFENSIVĂ cadrul cărei se va folosi întreaga gamă a procedeelor de ducere a operaţiilor care permit, în final, într-o conjunctură poliitico-militară favorabilă, realizarea integrală a obiectivului politico-strategic al războiului de apărare a ţării.

RIPOSTĂ w acţiune ofensivă în cadrul apărării prin care se urmăreşte

OFENSIVĂ nimicirea inamicului pătruns în interiorul apărării şi refacerea acesteia pe aliniamentul iniţial (riposta de răspuns) sau lovirea inamicului în faţa limitei dinainte apărării (riposta de prevenire).

RIPOSTĂ principiul fundamental al acţiunilor militare în caz de

OPTIMĂ război, similar „apărării flexibile şi ripostei ofensive decisive”.

RITM viteza cu care se realizează, într-o perioadă dată anumite acţiuni de luptă sau alte activităţi militare.

RUPEREA acţiune de luptă dusă împotriva unui inamic aflat în

APĂRĂRII apărare, incluzând executarea loviturii frontale şi crearea unei breşe în dispozitivul apărării inamice, de o lărgime şi adâncime care să permită dezvoltarea ulterioară a ofensivei în adâncime şi spre flancuri.

S

SCOPUL constă în respinderea, capturarea ori nimicirea grupărilor

STRATEGIC de forţe ale agresorului şi anihilarea capacităţii combative

GENERAL AL a acestuia, urmărindu-se asigurarea suveranităţii

APĂRARII naţionale, independenţei şi unităţii statale, integrităţii

ARMATE A teritoriale a ţării. ŢĂRII

SECURITATEA starea în care trebuie sa se găsească statul român pentru NAŢIONALĂ a putea să se dezvolte liber şi să acţioneze neîngrădit pentru promovarea intereselor fundamentale ale României.

SIMULARE formă de instrucţie specifică pregătirii comezilor şi

CONSTRUCTIVĂ comandamentelor de la nivel batalion până la nivel teatru de operaţii, ce se realizează prin antrenamente de stat major/aplicaţii de comandament asistate de calculator.

SIMULARE ÎN forma de instrucţie cea mai complexă care asigură TEREN CU instruirea militarilor, subunităţilor, comenzilor şi

TRUPE comandamentelor prin exerciţii şi aplicaţii tactice în teren, în cele mai apropiate condiţii impuse de câmpul de luptă modern, fără utilizarea muniţiilor de război.

SIMULARE formă de instrucţie care asigură instruirea militarilor şi

VIRTUALĂ echipajelor prin utilizarea machetelor electronice ale tehnicii de luptă.

SISTEM ansamblul de elemente (principii, reguli, forţe etc.)

dependente între ele şi formând un întreg organizat care face ca o activitate practică să funcţioneze potrivit scopului urmărit.

SISTEM DE ansamblul de metode, tehnici şi instrumente, asociat cu

CONDUCERE procedurile informaţionale, decizionale şi organizatorice specifice metodelor şi tehnicilor integrate în cadrul sistemului.

SISTEMUL DE parte componentă a sistemului de conducere a armatei, CONDUCERE A destinată să facă posibilă conlucrarea şi cooperarea cu FORŢELOR structurile de comadă din compunerea Ministerului

TERESTRE Apărării Naţionale, Statul Major General, statelor majore ale categoriilor de forţe ale armatei, celorlalte elemente ale Sistemului Naţional de Apărare, administraţiei locale, precum şi din cea a partenerilor de coaliţie sau de misiuni comune.

SISTEM DE ansamblul acţiunilor tuturor categoriilor şi sistemelor de

LOVIRE armamente şi mijloace de lovire, executate în scopul producerii de pierderi, diminuării puterii de luptă şi anihilării acţiunilor inamicului, în spaţiul terestu, aerian, maritim şi fluvial.

SPRIJIN orice ajutor sub formă de bunuri şi/sau servicii, sprijin

LOGISTIC tehnic sau nontehnic, acordat de o parte ce oferă sprijin către o parte primitoare.

SPRIJINUL CIVIL totalitatea activităţilor şi măsurilor luate de forţa de intervenţie în scopul favorizării asistenţei şi sprijinului reciproc între structurile militare şi orice organism civil în procesul de planificare/pregătire sau aplicare a resurselor necesare pentru a răspunde consecinţelor unor situaţii critice, de urgenţă, de natură civilă sau în caz de atac, incluzând situaţiile de urgenţă în planul securităţii naţionale.

SPRIJINUL operaţie care asigură sprijinirea unei mişcări organizate

INSURGENŢILOR care urmăreşte unui grup constituit pe calea subversiunii şi a conflictului armat.

STANDARD o valoare, o unitate fizică sau o noţiune abstractă, stabilită şi definită de autoritate, obicei sau acord comun pentru a servi ca referinţă, model sau regulă în măsurile cantitative sau calitative, în stabilirea practicilor ori procedurilor, sau în evaluarea rezultatelor.

STANDARD DE normele, baremele, criteriile sau ansamblurile de norme

INSTRUCŢIE care sunt stabilite pentru un agent al acţiunii militare sau pentru o structură militară care îndeplinesc o acţiune/ activitate/misiune specifică în anumite condiţii.

STANDARDE cele ce fac referinţă asupra practicilor, procedeelor,

OPERAŢIONALE metodelor, cu aplicabilitate imediată sau viitoare. Ele privesc: aspectele de natură conceptuală, doctrinară, tactică şi tehnică; antrenamentele, pregătirea şi perfecţioanrea; precizările organizatorice, rapoartele, schemele, hărţile ş.a.

STANDARDIZARE procesul de formulare (elaborare), punere de acord şi introducerea standardelor în cadrul Alinaţei NATO în scopul dezvoltării capacităţii ei militare.

STANDARDIZA^ procesul dezvoltării conceptelor, procedeelor şi

REA LOGISTICĂ proiectelor de a realiza şi menţine nivelurile cele mai adecvate de compatibilitate, interoperativitate, interschimbabilitate şi a calităţii de a fi comune în domeniul operaţiilor, administraţiei şi materialelor.

STAREA DE situaţia în care sistemul social-global, în totalitate sau

CRIZĂ numai parte din el, este marcat de convulsii, de ameninţări interne şi externe sau mixte, precum şi de stagnarea şi perturbarea vieţii societăţii, toate acestea punând în pericol valorile naţinale şi democraţia constituţională.

STAREA DE cadrul de normalitate relativă, în care viaţa economică,

PACE politică, militară etc. Îşi urmează cursul firesc.

STATUI. MAJOR structură de comandă, de concepţie şi execuţie care AL FORŢELOR răspunde de întrebuinţarea forţelor şi mijloacelor din TKRKSTRK subordine, funcţionează la pace, în situaţii de criză şi război şi se subordonează ierarhic Statului Major General.

STATIONARKA acţiunea pe care o desfăşoară structurile militare atunci când nu execută operaţii

militare, nu se deplasează şi nu sunt în dispozitiv de luptă.

STRATEGIE ansamblul de concepte şi măsuri ce constau în aplicarea resurselor naţionale, diplomatice; economice şi militare, pentru îndeplinirea obiectivelor politice.

STRATEGIILE programele generale/direcţiile de acţiune/alocare a INSTRUCŢIEI resurselor pentru executarea intrucţiei pe termen mediu/ ARMATEI lung. Ele stabilesc obiectivele, definesc responsabilităţile, asigură ghidul/îndrumarile/metodologiile şi repartizează prioritătile.

STRATEGIILE programele generale/direcţiile de acţiune/alocare a INSTRUCŢIEI resurselor pentru executarea intrucţiei pe termen mediu/ FORŢELOR lung; sunt elaborate de către Statul Major General al

TERESTRE Forţelor Terestre şi sunt materializate prin regulamente, instrucţiuni, dispoziţii şi manuale ce cuprind prevederi generale sau specifice privind executarea instrucţiei.

SUBSISTEMUL totalitatea forţelor şi mijloacelor care au misiunea de a DE PROTECŢIE asigura securitatea sistemului de conducere şi vizează sursele, mijloacele de prelucrare, suporţii, legăturile, depozitele, locurile de ahşare-exploatare şi purtătorii de informaţii.

SUBSISTEMUL totalitatea forţelor şi mijloacelor din structura Forţelor INFORMAŢIONAL Terestre cu ajutorul cărora sunt obţinute, transmise, prelucrate, depozitate şi exploatate informaţii, date şi semnale.

SUBSISTEMUL totalitatea comandamentelor de mari unităţi (la pace şi INFRASTRUCTURII în situaţii de criză) şi a punctelor de comandă.

SUBSISTEMUL cuprinde modulele (centrele operaţionale) ale punctelor MANAGERIAL de coamdă (comandamentelor), reguli de funcţionare şi relaţiile dintre acestea.

SUFICIENŢA structură de potenţial, staţial şi temporal, subsumată ACTIVĂ A nivelului global, cu coeficient al stării de resursă activă,

APĂRĂRII în măsură să asigure riposta armată pentru respingerea din primele momente ale unui tip de agresiune pe o direcţie strategică.

SUFICIENŢA concept strategic fundamental care reflectă opţiunea PENTRU statului român în domeniul apărării, semnifică tipologia

APĂRARE exclusiv defensivă a războiului ca model strategic

(PRINCIPIU) preconizat pentru respingerea unei agresiuni şi desemnează starea de normalitate a Sistemului Naţional de Apărare, fără a reprezenta o ameninţare la adresa altor state.

SURPRINDEREA are rolul de a impune adversarului voinţa proprie, de a realiza superioritatea în punctul şi la momentul hotărâtor. Odată realizată, paralizează capacitatea de reacţie cel puţin la nivelul eşalonului direct afectat, inclusiv la nivelul conducerii, care nu mai reacţionează în timp oportun pentru contracararea adversarului.

SURPRINDEREA ansamblul măsurilor şi acţiunilor adoptate de conducerea STRATEGICĂ politico-militară în cadrul unei operaţii strategice sau uneori al unei campanii ori a unei etape a războiului, în aşa fel încât acţiunile politice, militare, diplomatice, economice, pshilogice etc. atât în ceea ce priveşte conţinutul (substanţa), cât şi în ceea ce priveşte locul, momentul, amploarea, procedeele practice de acţiune

(realizare), să aibă un caracter neprevăzut pentru adversar.

Ş

ŞEDINŢĂ w formă de organizare a procesului de instrucţie ce asigură

PRANCTICĂ formarea deprinderilor individuale de bază ale luptătorilor, a deprinderilor colective specifice grupelor/ similare, a capacităţii de rezolvare a situaţiilor complexe, neprevăzute, în timp oportun a evenimentelor apărute în dinamica luptei.

ŞEDINŢA formă de organizare a procesului de

instrucţie care se

PRACTIC- w execută, de regulă, întrunit cu subunitatea şi unitatea APLICATIVĂ urmărindu-se, pe lângă realizarea obiectivelor punctuale, în mod deosebit, închegarea acţiunilor subunităţilor şi unităţilor, precum şi intruirea integrată de la cel mai mic nivel, respectiv echipa/postul/echipajul/similare, până la nivelul batalionului/similare.

ŞEDINŢĂ ^ formă de organizare a procesului de instrucţie care asigură

TEORETICĂ însusirea conceptelor, a limbajului militar, a informaţiilor despre acţiunile ce urmează să fie învatate, a cunoştinţelor necesare formării atitudinilor şi sentimentelor superioare.

T

TEHNICA DE ansamblul de reguli specifice, procedee şi instrumente CONDUCERE prin care se soluţionează concret probleme ce decurg din funcţiile conducerii.

TERORISMUL un act violent premeditat, realizat de organizaţii conspirative cu caracter distructiv sau de persoane individuale, împotriva unor demnitari, a unor obiective (instituţii) politice, economice, ştiinţifice, militare, culturale, diplomatice, în scopul răzbunării, obligării ţintei să adopte o conduită convenabilă teroriştilor, sensibilizării opiniei publice în legătură cu o cauză anumită, al erodării stabilităţii politice şi satisfaceerii unor revendicări.

TRANSPORTUL deplasarea organizată a structurilor militare pe vehicule, altele decât cele din dotarea proprie.

TRANSPORTURILE activităţile desfăşurate pentru deplasarea materialelor din LOGISTICE sursele de aprovizionare până la luptător (tehnică), precum şi a celor care prisosesc pe câmpul de luptă, către înapoi, în locurile stabilite din timp.

U

UNITATEA stabilirea precisă a atribuţiilor şi responsabilităţilor pe

CONDUCERII ŞI sfere şi niveluri de activitate,

începând cu structurile cele RĂSPUNDERII mai mici până la structura care coordonează sistemul de instruire al armatei.

UNITATEA DE derivă din principiul unităţii de comandă şi cere ca în EFORT fiecare operaţie militară toate mijloacele să fie întreptate spre un obiectiv comun.

Z

ZONĂ DE în spaţiul geografic care include statele şi regiunile a căror

INFLUENŢĂ evoluţie influenţează direct situaţia din ţara noastră şi cuprinde în esenţă ţările vecine şi Marea Neagră.

ZONĂ DE spaţiul din afara zonei de responsabilitate care cuprinde

INTERES factori ce pot influenţa pregătirea şi desfăşurarea acţiunilor militare.

ZONĂ DE spaţiul în care comandantul unei unităţi are

RFSPONSARTT T responsabilitatea pentru amenajarea genistică, controlul TATF deplasărilor şi conducerea acţiunilor militare ale forţelor subordonate, precum şi autoritatea necesară pentru măsurile de rezolvare ale acestora.

ZONĂ w porţiune de teren destinată marilor unităţi strategice sau

LOGISTICĂ operative pentru dispunerea şi desfăşurarea acţiunilor marilor unităţi, unităţilor şi formaţiunilor de logistică, stabilirea responsabilităţilor în folosirea căilor de comunicaţie, organizarea folosirii posibilităţilor logistice ale zonei şi aplicare unitară a măsurilor de protecţie.

CUPRINS

PREFAŢĂ

BAZELE RĂZBOIULUI INFORMAŢIONAL

Era informaţiei

RĂZBOIUL INFORMAŢIONAL DEFENSIV OPERATELE INFORMAŢIONALE. CÂTEVA REFLECTE OPERAŢIONALE SISTEMUL SISTEMELOR

ATACUL INFRASTRUCTURE CRITICE

RĂZBOIUL NEOCORTICAL UN CONCEPT PENTRU VETOR

OPERATELE INFORMATIONALE PERSPECTIVA NATO..!!

A INFORMA, CHIAR ÎN CONDIŢE DIFICILE

SIGURANŢA INFORMAŢIONALĂ

EXPLOZIA TEHNOLOGIEI INFORMAŢIEI

Dimensiunea 1: Conţinutul

Dimensiunea 2: Intervalul de timp

Dimensiunea 3: Accesibilitatea

Dimensiunea 4: Gradul de încredere

Dimensiunea 5: Calitatea Dimensiunea 6: Cantitatea

STUDIUL GERMANO-OLANDEZ DESPRE RĂZBOIUL INFORMAŢIONAL

RĂZBOIUL INFORMAŢIONAL PROBLEME şi PERSPECTIVE

EXCURS IN SPAŢIUL CONCEPTELOR

RĂZBOIUL INFORMAŢIONAL. ABORDARE TEORETICĂ

ŢINTE ŞI ELEMENTE ALE UNUI ATAC INFORMAŢIONAL

INFRASTRUCTURILE CRITICE ÎN RĂZBOIUL INFORMAŢIONAL

PROBLEMATICA EVALUĂRII AMENINŢĂRILOR RĂZBOIUL INFORMAŢIONAL SI LEGISLAŢIA INTERNAŢIONALĂ

VULNERABILITĂŢI ALE TEHNOLOGIEI INFORMAŢIEI

OPERAŢIILE INFORMATIONALE UN MIJLOC DE DESCURAJARE STRATEGICĂ

DELIMITĂRI SI DIFERENTE

FORMELE DEFENSIVE SI OFENSIVE ALE OPERAŢIILOR INFORMÀTIONALE

MANAGEMENTUL PERCEPŢIILOR SI FACTORUL UMAN 1

ELEMENTE ALE UNEI STRATEGII DE INFLUENŢARE

SIGURANŢA INFORMAŢIONALĂ EXPERIENŢA CANADIANĂ
RĂZBOIUL INFORMAŢIONAL PROBLEME DE SECURITATE '
RĂZBOIUL CUNOAŞTERII
REVOLUŢIA INFORMAŢIONALĂ
Anexa 1: NETWORK CENTRIC WARFARE
Anexa 2:
1. RĂZBOIUL INFORMAŢIILOR A DEVENIT DEJA O REALITATE A CÂMPULUI DE LUPTĂ MODERN
2. CARACTERISTICI ALE DINAMICE RESURSELOR INFORMATIONALE
3. OPERAŢIILE INFORMATIONALE
4. OPERAŢIILE INFORMAŢIONALE PENTRU SITUATIILE DE URGENTA
5. RĂZBOIUL MEDIATIC
6. RĂZBOIUL ELECTRONIC
7. TERORISMUL INFORMATIC
Anexa 3: Resurse URL (Uniform Resourse Locator)
Dicţionar

24 Dixon, p. 28

43 J. de Rosnay, The Macroscope, Harper & Row, Publishers, New York, 1979.

44 Alvin Toffler, Război şi anti-război, Ed.Antet, 1995.

65 În documentul FM 100-6 „Information Operations", 27 aug. 19%

66 „Joint Doctrine for Information Operations", *Joint Pub3-\3*, oct. 1998

98 „Indian Government Concerned over Lack of E-Comercc Capabilities", *Telecomworld-Wire*, 10.05.1999.

99 Alvin şi Heidi Toffler, „Beyond Future Shock: Conspiracies, the Media and the War for the World* s Mind", Los Angeles Times Syndicate, 15.06.1999.

1 100 Richard Szafranski, „Toward a Theory of Neocortical Warfare:

Pursuing the Acme of Skill", *Military Review*" 11.1994.

* Agenţia serviciilor de apărare a comunicaţiilor

109 John Deutch, „Oral evidence to US Senate Committee ol Government Affairs”, The *Times*, 26.06.1996.